(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 February 2001 (15.02.2001)

PCT

(10) International Publication Number
WO 01/11812 A2

(51) International Patent Classification[7]: H04L

(21) International Application Number: PCT/US00/21586

(22) International Filing Date: 8 August 2000 (08.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/147,869 9 August 1999 (09.08.1999) US
60/147,951 9 August 1999 (09.08.1999) US

(71) Applicant and
(72) Inventor: SUDIA, Frank, W. [US/US]; 237 Banks Street, San Francisco, CA 94110 (US).

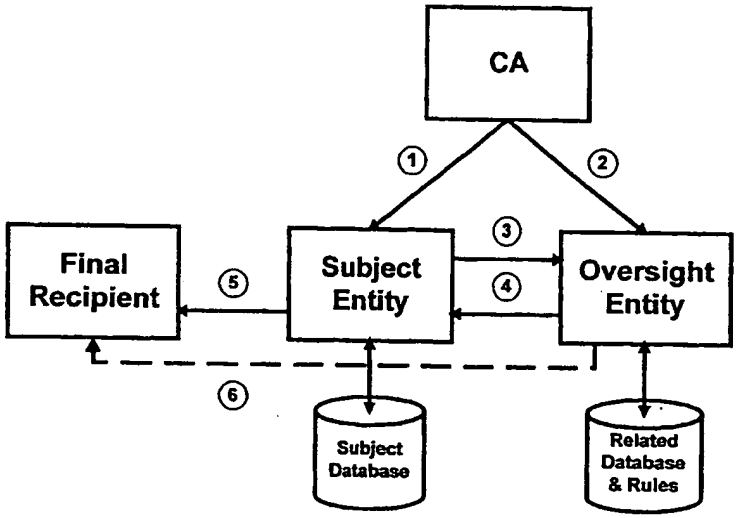
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DISTRIBUTED RULE ENFORCEMENT SYSTEMS



(57) Abstract: A method is provided for communicating authenticated information concerning a digital public key certificate. A hash-tree data structure is created containing a pre-defined list of possible information, such as authorizations, restrictions, privileges, or validity period notices. The list items may include text and coded values. Each list entry is prefixed with a different random data (blocker) value that is securely stored and infeasible to guess. Each list item is hashed to produce a leaf hash, the leaf hashes are combined to produce a hash tree, and the root node of said tree is embedded into a digital certificate or message that is signed using a private key. In response to a request for authenticated information concerning a digital public key certificate, the certificate authority releases the relevant list item, its blocker value, and other hash values sufficient to authenticate the list item using the root node embedded in the digital certificate.

WO 01/11812 A2

DISTRIBUTED RULE ENFORCEMENT SYSTEMS

BACKGROUND OF THE INVENTION

1.1. Cross Reference to Related Applications

The present application claims priority under 35 U.S.C. § 119(e) of U.S. Provisional Patent Applications Nos. 60/147,869 and 60/147,951, both filed on August 9, 1999, the disclosures of which are expressly incorporated by reference herein in their entireties.

1.2. Field of the Invention

This invention pertains to secure and efficient systems for controlling access to data and network resources, and providing privacy and authentication of data, in electronic commerce on the Internet.

More particularly, in an electronic trading network, digital certificates can be used to declare and enforce use condition specifications, which can be checked by one or more entities in a multi-stage transaction matching, clearing, and settlement system.

In addition, the approval of a transaction can be made conditional on securing the consent of a "reference party," which maintains a synchronized parallel account database.

SUMMARY OF THE INVENTION

The present invention constitutes a system to efficiently create and enforce use conditions for electronic transactions, especially in a global financial market system.

1.3. Related Art

1.3.1. U.S. Patents

Asay, et al, US 5,903,882, May 11, 1999, Reliance Server for Electronic Transaction System

Brickell et al, Adaptive Multi-Step Digital Signature System and Method of Operation Thereof, US 5, 867,578

Fischer, Public Key/Signature Cryptosystem With Enhanced Digital Signature Certification; US Nos. 5,214,702; 5,005,200; and 4,868,877

Fischer, 5,311,591 Computer System Security Method and Apparatus for Creating and Using Program Authorization Information Data Structures

Fischer, 5,412,717 Computer System Security Method And Apparatus Having Program Authorization Information Data Structures

Howell, 5,450,593 Method and System for Controlling Access to Objects in a Data Processing System Based on Temporal Constraints

Janis, 5,263,158 Method and System for Variable Authority Level User Access Control in a Distributed Data Processing System Having Multiple Resource Manager

Kravitz, US 6,029,150 Payment and Transactions in Electronic Commerce System

Marino, US 5,530,758 Operational Methods for a Secure Node in a Computer Network

Sudia US 5,659,616 Method for Securely Using Digital Signatures in a Commercial Cryptographic System

Sudia, US 5,799,086 Cryptographic System and Method with Key Escrow Feature

Sudia et al, US 5,825,880 Multi-Step Digital Signature Method and System

Sudia et al, US 5,995,625 Electronic Cryptographic Packing

1.3.2. Foreign Applications

Frankel at al, WO 99/42965, Computer-Based Method and System for Aiding Transactions

Sudia et al, WO 96/02993, Method for Securely Using Digital Signatures in Commercial Cryptographic System (CIP)

See also, Sudia, WO 00/22787: Method, System, and Computer Program Product for Providing Enhanced Electronic Mail Services.

1.3.3. Other References

Johnston et al, "A Use-Condition Centered Approach to Authenticated Global Capabilities: Security Architectures for Large-Scale Distributed Collaboratory Environments" Lawrence Berkeley National Laboratory, dated January 14, 1997.

Johnston et al, "Distributed, Collaboratory Experiment Environments (DCEE) Program: Overview and Final Report," Lawrence Berkeley National Laboratory, February 1997.

Aiken et al, Public Key Infrastructure for DOE Security Research," Findings from US Dept. of Energy Joint Energy Research / Defense Programs Computing Related Security Research Requirements, Workshop II, Dec 11-13, 1996, Albuquerque, NM.

Ankney, R. and F. Sudia, ANSI X9.45 "Enhanced Management Controls Using Attribute Certificates." American Bankers Association

Ankney, R., "Certificate Management Standards," April, 1999.

Blaze at al, "Decentralized Trust Management" [Policy Maker], IEEE Conference on Security and Privacy, Oakland, CA May 1996.

Dusse et al, S/MIME Certificate Handling, Internet Draft, May 5, 1997.

Dusse et al, S/MIME Message Specification, Internet Draft, May 5, 1997.

ECMA-219, "Authentication and Privilege Attribute Security Application with Related Key Distribution Functions," 2nd Edition, European Computer Manufacturers Association, March 1996.

ITU-T Recommendation X.509, "The Directory: Authentication Framework," 1997.

ITU-T Recommendation X.509, ISO/IEC 9594-8: "Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks" ("X.509 Version 4," Draft Revised, 2000)

PKCS #7: Cryptographic Message Syntax Standard, RSA Data Security, Inc., June 3, 1991.

Zurko et al, "Separation of Duty in Role-Based Environments," The Open Group Research Institute, Cambridge, MA. (before 6-6-97)

Other exemplary embodiments and advantages of the present invention may be ascertained by reviewing the present disclosure and the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is further described in the detailed description which follows, in reference to the noted plurality of drawings by way of non-limiting examples of certain embodiments of the present invention, and wherein:

FIG 1 shows a general overview of the certificates, participants, and process flow for distributed rule enforcement for an electronic exchange market. As elsewhere in this disclosure, the rules and use-conditions are shown being checked by the clearinghouse. However, since all the relevant certificates are generally available to all entities, it is

possible to check these conditions at other stages in the process as well. Elements shown as dotted outlines represent additional parties commonly found in exchange trading systems, but which are not essential for understanding or implementing the system.

FIG 2 shows the general method of use (preferred embodiment) in which a user transaction (order) message is sent to an exchange and matched, whereupon the exchange creates and signs an execution report message, which is sent to the clearinghouse, usually along with copies of the underlying user transaction messages and user certificates. The clearinghouse then validates the parties and the transaction and sends trade confirmation messages back to the parties.

FIG 3 shows the transaction elements seen by the clearinghouse, and some tests that the clearinghouse can perform to enforce trading rules as contemplated by this invention. The specific tests are detailed in the accompanying text.

FIG 4 shows additional tests and processing performed by the electronic market server and/or the clearinghouse to (a) enforce any trading restrictions or limitations that may apply to the participant or products traded by the participant, and (b) transfer the product using a specified means, such as an electronic registry system (transfer agent or securities depository) or physical processing agent (fulfillment service).

FIG 5 shows additional tests and processing performed by the electronic market server and/or the clearinghouse to enforce any restrictions relative to the source of funds used to settle the transaction. This may include the requirement of a warranty as to the origin or destination of funds, to be made by a paying bank or institution, relative to funds being received from or paid to that bank or institution. This method can be used with respect to the source and destination of securities, commodities, or other products being traded in an electronic market. Such product-oriented restrictions would be applied within the messages sent to central depositories, transfer agents, fulfillment services, and the like.

FIG 6 is a schematic representation of a general framework for a distributed accounting system;

FIG 7 is a schematic representation of a multi-signature transaction approval process (prior art);

FIG 8 is a schematic representation of a required co-signer transaction approval process (prior art);

FIG 9 is a schematic representation of a required confirmer transaction approval process (prior art);

FIG 10 is a schematic representation of an exemplary multi-entity oversight architecture (present invention).

DETAILED DESCRIPTION OF THE EMBODIMENTS OF THE INVENTION

2. Distributed Market System Overview

In a distributed electronic market system, especially one for securities, there is a strong need to control who can do what, and to prevent transactions from taking place that are not in accord with the relevant rules. The most common sources of such rules are local terrestrial governments, industry trade associations, and the operators of the exchange, brokerage, matching, clearing, settlement, and payment systems.

Participants may utilize a trade matching system to efficiently create contracts that bind themselves and another party to perform some transaction, such as the purchase or sale of a product. The perceived quality of service to the participant will depend in part on the rules and remedies that can be, and are in fact, enforced against counterparties in that system, in case any problems arise.

For economy of expression and to avoid confusion, the following definitions will be used:

1. Product means goods, services, real estate, transportation, software, information, intellectual property rights, money, credit, foreign exchange, financial instruments, scrip, allocations or allotments, investment opportunities, admission to events, advice, barter, employment opportunities, charitable subscriptions or projects, computer time, communication network capacity; oil, natural gas, and electric power transmission facilities; any associated or bundled taxes, commissions, and fees; requests for quotations (RFQs) and requests for proposals (RFPs); plus all other things, rights, capabilities, liabilities, opportunities, privileges, etc., tangible or intangible, now or hereafter capable of being listed for trading on an electronic exchange trading system.

2. Exchange means the system of computerized and/or human processes that lists products for sale, purchase, or barter in an auction market, publishes bid/ask prices, receives incoming orders to buy, sell, or exchange, matches those orders with each other to produce enforceable contracts, and reports the trade back to the participants, their brokers, and/or the entities appointed to clear and settle the transaction, and (usually) publishes the price and size of the transaction so that others may have the benefit of knowing the most recent price at which the product traded.
3. Market system means the entire ensemble of entities, parties, rules, electronic systems, security procedures, and the like needed to accomplish the trading process in a secure and reliable manner, and to maintain and properly care for the assets before and after the trade.
4. Order means a binding offer to buy or sell a product.
5. Trade means a binding contract to buy or sell a product.
6. Trading system means any software, hardware, facilities or personnel relevant to any aspect of the trading process, including portfolio management, pricing analytics, trade entry, order routing and processing, data feeds, etc. that may be utilized by any party in the market system. In common usage his term may, but often does not, encompass the exchange matching system itself.
7. Clearinghouse means a processing service which receives execution reports from one or more exchange market systems, identifies and verifies the parties, records the trade, sends a trade confirmation to the parties or their brokers, and sends instructions to settlement and/or payment services designated by the parties or their brokers telling those services to complete the process of transferring the underlying product.
8. Settlement means delivering, exchanging, or making the appropriate book entries to memorialize the payment for, and transfer of, an underlying product. In the case of financial securities, settlement may involve instructions to the buyer's bank to make payment to the seller, and instructions to a corporate transfer agent, or to a securities depository, such as Depository Trust Company (DTC), to transfer ownership of a specified number of security units.

9. Participant means any individual or entity interacting with an electronic market system, including customers, brokers, market makers, dealers, specialists, banks, insurers, regulatory agencies and personnel, system operators and managers, etc. A participant typically has a primary identification certificate and optionally one or more authorization certificates that define his identity, attributes, and trading rights or administrative rights. Depending on the market format, some participants may have more rights than others, as for example in a "dealer market" dealers have the right to post bid/ask prices while customers can only hit or take the posted prices, but cannot post prices of their own.

In a global electronic market system on the Internet, tens of thousands (and eventually millions) of independent computerized order-driven market systems may be anticipated, operating at different physical locations and/or network addresses, under the control of a wide variety of sponsors, each of which may handle unique products, or may provide competitive matching services for products that are similar to or identical to those offered on other exchanges.

This distributed rule enforcement system is concerned with providing means for allowing appropriate trading rules to be enacted and enforced across most or all such systems in a global distributed environment.

It is of course possible to locate the trade matching (exchange) server in a country with few or no relevant rules (such as Liechtenstein or the Bahamas). However, a participant attempting to trade or deal on such an unregulated exchange may not have the benefit of investor protections (such as minimum capital requirements for brokers, laws against insider trading, rules against short sales in falling markets, circuit breakers to suspend trading in the event of unusual market conditions, etc.)

This system cannot prevent such unregulated markets from being created, or force them to enact or enforce any particular rules. It is assumed that the participant seeking to trade will "shop around" the globe for the market(s) having the desired level of protection. However, when a market is located in a terrestrial region (country, state, province, etc.) that does have effective laws and enforcement governing the subject matter being traded, then this system can allow the regulatory entities in that region to effectively enforce

certain types of rules within their jurisdiction, for the benefit of all those who trade in the markets they supervise.

The underlying economic and regulatory premise of this invention is that there will be many markets, but relatively few clearinghouses. Hence, if the regulators can acquire jurisdiction over the clearing process, then this system will be highly effective, while permitting broad proliferation (scaling) of the number and kinds of markets, without causing increased regulatory problems. Indeed, this system will probably simplify and enhance the regulation of existing exchange markets, thereby increasing the level of protection those markets can provide to investors and traders.

The rule enforcement and use condition checking steps proposed herein can be performed at any stage of the trading process, including y the participant prior to initiating an order, by a broker or other intermediary (if any), by a trade routing service, by the exchange market, by the clearinghouse, or by the settlement or depository entities. Such checking and rule enforcement is preferably performed by the clearinghouse, however, since that can provide centralized control over possible abuses by market operators, while allowing nearly unlimited proliferation of market servers,

3. Discussion of Prior Art on Certificates

A public key certificate ("certificate") is an electronic message which makes an assertion about one or more useful facts, and has been signed by a trusted third party.

3.1. Types of Certificates

In the current state of the art, there are two major types of certificates:

a. certificates of identity, which bind the identity of a party with the public key attributed to that party, so the certificate and its public key can be used to authenticate messages electronically signed by that party, and

b. certificates of authority, which are long-lived representations that a given party has been granted the authority or privilege to perform or access some function by a sponsor, which typically is an employer or commercial entity to whose rules the party has subscribed.

Typically, there is a separation of functions between identity and authority certificates. A party may have multiple authority certificates each granted by different

sponsors, whereas it may prefer to have only one or a small number of identity certificates granted by a single certifying authority. It is relatively costly to perform the in-person identification needed to bind an individual to a public key, whereas once that has been done, the action of issuing the secondary authorization certificates can generally be accomplished on-line without personal presence, when other facts are in good order. Also once an individual has built up a collection of different authorities, it would be inconvenient if those all had to be contained in his identity certificate, because each time one permission needs to be revoked or modified, all other permissions would need to be reissued by the subject's other sponsors. Therefore, it is more convenient to "normalize" the permissions into a portfolio of separate authorization certificates each signed and issued by the relevant authorizing sponsor and linked to the identity certificate of the party.

3.2. Certificate Standards Documents

The use of public key certificates for identification and authorization of parties on electronic networks is extensively discussed in the following references:

- ITU X.509 Version 3, The Directory – Authentication Framework.
- ANSI X9.55 & 57, Public Key Certificate Management
- ANSI X9.45, Enhanced Management Controls Using Attribute Certificates
- Commercialization of Digital Signatures (Sudia & Ankney)
- US DoD, Message Security Protocol (MSP)
- ECMA, SESAME
- IETF, RFC 1424

3.3. Data Encoding

All data encoding in certificates will be performed using the Abstract Syntax Notation One (ASN.1) data description language as used in many standards. Each attribute or extension type will be assigned an object identifier in lieu of the text field label, and attribute values will be encoded either as primitive data types or as other object identifiers that have been pre-defined and published in an appropriate code book for the system.

3.4. Certificates and Extensions

For purposes of this discussion, the basic contents of an identity certificate are referred to as an "identity specification." These data elements will typically include: certificate version number, issuer name, issuer serial number, issuer signature algorithm type, subject name, subject public key, validity period, policy reference, issuer digital signature.

The policy reference can be any text or object identifier describing or pointing to a policy or set of terms and conditions pertaining to the manner in which the certificate was issued and the responsibility or liability, if any, of the issuer and subject – all digitally signed by the issuer.

Other certificate attributes and extensions have been defined in the various standards, especially X9.55, but they are not directly relevant to the discussion here.

The issuing certifying authority (CA) will generally have a similar certificate from its parent CA, containing similar information and digitally signed by that parent CA. The parent in turn may have another parent, or its certificate may have been issued by a Root CA, i.e., on that has no certificate, but which has made its public key widely available through physical delivery in an uncertified form. The general framework for issuance of identity certificates by CAs is well defined in the prior art.

For further purposes of this discussion, the set of attributes or extensions that state the authorizations and restrictions of a given party, as defined in ANSI X9.45 (and related patents), are referred to as an "authority specification." As noted, this authority specification may be included in the same certificate as the party's identity specification, but more commonly, for ease of issuance and revocation, it will be placed in a separate secondary authority certificate.

In a secondary authorization certificate there is a need to refer to the primary identity certificate that the recipient must use to identify the party having the stated authority. Most commonly this is done by listing the issuer name and certificate number of the relevant identity certificate as a data field in the authority certificate. Or alternatively, it might be accomplished by directly reproducing all or part of the full identity specification from the base certificate. Whether the information is given in full, or

by reference using a pointer (such as the issuer name and serial number), such identity information will in both cases be referred to as the "identity specification" of the authority certificate.

3.5. Enforcement by Recipient

A common theme underlying the field of authorization certificates is that the enforcement of the conditions stated in the authorization certificate must be performed by the recipient of the message (who is also variously referred to as the verifier or the relying party). To effectuate this scheme, the recipient must be under contract with the entities that issued the certificate(s), or else bound by an effective terrestrial law, treaty, or custom defining his duties. Otherwise he might not bother to verify the authority elements contained in the certificates prior to relying on the transaction, and then claim to have been misled.

The distributed rule enforcement system defined herein continues this requirement, with the understanding that (unlike a pure contracting system, where the recipient may be anyone in the world) the most important recipients will be markets, clearinghouses, and payment processors, who are relatively few in number and comparatively easy to regulate and audit.

Of course the initiating participant (sender) and any intermediary along the way can also check the validity of a transaction against the authorizations and restrictions specified in the relevant certificates. However, from a legal and banking standpoint, the best point at which to perform effective checking is generally right before the final transfer or reliance takes place.

3.6. Filters, Macros and UDFs

In the field of authorization certificates, the pertinent requirements may be defined as "filters" or composite statements containing logical operators, including AND, OR, NOT, multiple levels of parentheses, arithmetic functions, and pattern matching rules. The rule will be considered to be met if the conditions it implies are satisfied in at least one way.

When the same condition, variable, or value must be repeated in the same specification, a short tag may declared and defined as standing for the given condition,

requirement, variable or data value, which can then be used in the filter for economy of expression, being expanded in full prior to being interpreted and evaluated. In one embodiment, the ampersand '&' character may be used as a prefix to identify a text "macro" variable.

When an evaluation of a condition requires the substitution of parameters into a function or expression, another convention is to declare a user defined function (UDF). This can operate like a macro, in the sense that it will be substituted and expanded in full prior to being interpreted, with the added property that fixed or variable data quantities can be passed in as parameters

The use of filters (see ANSI X9.45), macro expansion, and user defined functions is well known in the art of computer programming. They are mentioned here only to illustrate that the specification of logical conditions and rules in certificates is not limited to simple assertions, and can be quite sophisticated. Indeed, one could also embed a short computer program (e.g., written in Java) into a certificate, thereby making the evaluation of the condition even more generalized.

3.7. Revocation

As is well known to those skilled in the art, certificates (with very few exceptions) are subject to revocation by their issuers at any time, based on receipt of information that makes the information represented in the certificate inaccurate or unreliable. Typically, a certificate will be identified by its issuer name and certificate serial number. Issuers desiring to revoke certificates will publish the relevant serial numbers on a list, known as a certificate revocation list (CRL), containing the issuer's name and signed by the issuer. These CRLs are then made available to individuals, firms, and directory services, which in turn republish this information in broadly available form, such that anyone desiring to learn the status of a given certificate may do so by inquiring to the appropriate service. This subject is covered extensively in US 5,903,882, and will not be further discussed. For purposes of this system, it is assumed that all users will check the status of all certificates prior to relying on them.

3.8. Enhanced Legal Effect

Special additional techniques are required to assure that persons using the certificates defined herein (a) will be legally bound, even in the case of third party recipients, and (b) will have adequate financial guarantees. Such techniques are discussed in US 5,903,882 and US 5,995,625.

We need not discuss these techniques in this application, except to note that similar results can be achieved in a straightforward manner by adding those features to the distributed rule enforcement system described herein.

4. Summary of the Invention

This invention specifies (a) new certificate attributes suitable for assigning various types of trading rights and privileges to parties and entities in a global electronic market system; (b) new types of certificates to be attached to markets, products, and rules; and (c) new technical processes whereby these certificate attributes can be verified and compared by appropriate entities in the course of a transaction in an electronic market system to determine whether the rules have been followed and reject transactions that are not in accord with the rules.

First the prior art concepts of identity, authorization/restriction, and reliance specifications are reviewed. Then the following novel concepts will be described and developed:

- Market Certificate, issued by a regulator to a market (or by a bank under the authority and direction of a regulator) to identify:
    1. The market, its sponsors and general rules, nationality and jurisdiction, identity of regulators, procedures for registering complaints, available remedies, etc.
    2. Allowed participants and applicable trading rights of the given participant.
    3. Allowed products or product classes.
    4. Capabilities (if any) for performing real time checks of external limitation specs for specific product types in participant certificates.
    5. Allowed market formats (e.g., continuous double auction, dealer market, specialist market, one-price auction, Dutch auction, Vickrey [2nd price] auction, broker call auction, anonymous preference optimization, etc.)

6. Allowed order matching rules (e.g., traditional execution control rules such as stop, limit, AON, FOK, at the close, at the open, etc., as well as various novel methods of seeing a suitable match, including rules based on multi-factor non-linear optimization, fuzzy logic, and the like). This will also include customer selectable instructions for splitting and grouping of an order, including partial order fills, allocation preferences, etc.
7. Allowed or preferred trade routing rules, such as instructions to seek a match on a local order matching system for a certain period of time, and if unsuccessful, or if prices are moving in a certain direction, to reroute the order to another market and seek an execution there.
8. Special matching rules (if any) to be followed upon opening or closing trading in certain products, etc., depending on the market format.
9. Internal trading context rules that are enforceable based on knowledge of immediate or recent trading conditions within a given market (e.g., prohibition of short sales on downticks, circuit breakers for large downward price movements in individual products or market indices, maximum bid/ask spreads, etc.
10. External trading context rules that require knowledge of trading conditions or other events outside the given market in which they are being enforced (e.g., price movements of the same or other products on other markets).
11. Other external rules of possible interest (such as rules against trading on inside information or requiring accurate reporting of company financial information) which cannot be enforced by technology, but which may be of interest to participants.
12. Intermarket trading groups in which the market participates. (Note: Each intermarket trading group will also have a certificate assigned to it, identifying its product groups and intermarket pricing rules. The market's certificate may refer to the intermarket trading group certificate.)
13. Source of funds rules, such as a restriction on the sources of funds that can be used to pay and settle transactions.

14. Information regarding who (which entities, e.g., market, clearinghouse, bank) will enforce market rules, whether any programmable trusted devices are used to enhance the reliability of the rule enforcement process, and if so who has administrative control of such devices.

- Product Certificate, issued by a regulator to define and enable a specific product, including its textual and data description (data format, rule set, terms and conditions, warranties, etc.), approved trading formats and rules (including acceptable matching rules, possible limits on bid/ask spreads, types of allowed participants, e.g., dealers or accredited investors only, etc.), how the ownership interest may be transferred (such as via instructions to a securities depository, transfer agent, or fulfillment service, etc.), restrictions on source/destination of funds/delivery including warranty requirements, external context restrictions, and who (if anyone) may modify the data description, etc.

  Due to accelerating product innovation in many areas, it may become desirable to allow privileged participants to modify product descriptions and trading/matching rules to sustain a dynamic market.

- Rule Certificate, issued by a regulator to a define and enable a specific matching rule or trade routing rule, including its textual and data description (pseudo-code, executable code, terms and conditions, etc.), market formats in which it may be used, approved methods of use, who may modify it, etc.

- Participant Certificate, issued by any reputable CA, such as a bank, preferably under authority and direction from a regulator or market, attesting to the identity, attributes, and qualifications of an individual user to participate in allowed trading markets, including allowed products and allowed trading and matching rules. As noted, allowed markets, allowed products, trading rights, and trading/matching rules may be grouped in different ways. The participant's certificate may contain an external limit specification, directing the market or clearing agent to verify that the participant has not exceed his trading limits (which may apply only to a small range of products). It may also contain a payment and settlement specification, identifying a bank account to be used as a source or destination of funds for

purchases or sales, and a custody account (such as with a securities broker) to be used as the source or destination of the ownership interest in products traded.

- Market Index Registration Certificate, issued by a regulator or market to fix the composition and method of calculation of a market index. This will be most relevant when the index is being used to enforce a rule, such as a circuit breaker. Also, when being traded in an index futures market, a market index can also be a product. However, unlike the product certificate, which would define allowed participants, matching rules, settlement procedures, etc., a market index certificate is primarily intended to provide an evidentiary definition of the index itself, for use in other calculations and processes. This will aid the proliferation of a wide variety of useful market indices in many areas other than financial securities.
- Data Feed Source Certificate, issued by a regulator to a source of current or historical price and transaction information. This certificate will define and register a source of price information, such as an active trading or dealer market, and may contain a public key which can be used to verify individual price feed messages (ticks) which have been timestamped and signed by the data source.
- Quote Source Certificate, issued by a regulator to a source of current price quotes, and may include a public key used to authenticate individual quote feed messages which have been timestamped and signed by the quote source. Since the entity certified is typically an active trading market, this is nearly the same as a market certificate. However, it may be preferable to limit use of the signature key of the market to signing completed transactions, while using a separate key for signing outgoing price quote messages.

Data source and quote source certificates are useful to verify the source and timeliness of signed price report or quote status messages that may be required for enforcing "external context" restrictions.

All these concepts are elements of the distributed rule enforcement system.

4.1. Specification Framework

4.1.1. Identity Specification

The long form identity specification will be the basis for a primary identity certificate. This certificate can, in theory, contain the additional specifications of authority, allowed markets, allowed products, trading rights, and product limitations. However, these items will typically be found in a secondary certificate that points to such a long form certificate using a short form identity specification (see next).

identity_certificate = SIGNED {
    certificate version number (=3)
    issuer name
    issuer serial number
    issuer signature algorithm type
    subject name
    subject public key
    validity period
    policy reference (text and/or OID)
    issuer digital signature
}

(Prior Art, ITU X.509 Version 3)

4.1.2. Identity Specification (Short)

A short form identity specification will be used in a secondary certificate to provide a reference to the primary identity certificate. The subject's name alone will generally be insufficient, since there may be multiple subjects with the same name, or it may be possible to procure a very low quality certificate that lists any subject name desired. Hence, the issuer name and serial number are generally be required, to provide assurance to the sponsor granting the authority that the quality of the underlying identity certificate will not be less than anticipated.

identity_spec = {

issuer name (of base identity certificate)
issuer serial number (of base identity certificate)
hash of subject public key (optional)
subject name

}

4.1.3. Authorization/Restriction Specification

An authority specification is intended primarily for a principal wishing to authorize an agent, subject to various substantive or security restrictions. This schema does not provide explicit support for references to certifications received from other sources. It is assumed that such certificates will simply be presented in their original form.

Where it is desired to represent that a party has a specified authority from another sponsor, such as a Series 7 broker license issued by the National Association of Securities Dealers (NASD), such a license would generally be represented by yet another secondary portfolio authorization certificate issued directly by or on behalf of the NASD. Of course, the issuer of an authorization could be the NASD (or possibly Merrill Lynch) and the role or title could be "Series 7 qualified broker".

```
auth_spec = {
    allowed role names = {{
        role name (e.g., signing as transfer agent)
        allowed signature purposes },
        repeat group ...}
    allowed document types = {{
        document type
        allowed content classes
        allowed monetary values },   -- note: might be zero
        repeat group ... }
    required cosigners = {
        K of N required
        list of identified public keys (hashes)
```

group specification }
technical restrictions = {
day of week (e.g., M-F)
time of day (e.g., 7AM-7PM -0600)
geographic location (e.g., GPS coordinates or net-seg address) }
substantive restrictions = {
pre-authorized counterparties (e.g., names or class description)
copy-to / confirm-to }
}

See ANSI X9.45 for related information.

4.1.4. Reliance Specification

reliance_spec = {
reliance in absence of signature guarantee (=0)
name of reliance (signature guarantee) service
signature guarantee price schedule (e.g., per $1000 of underlying)
parties that will pay signature guarantee fees CHOICE {
none, i.e., relying party must pay all fees
bill to account XXX of subscriber/sender/signer
bill to account YYY of employer or sponsor }
payment mechanism accepted (e.g., SET, CyberCash, Acquire)
}

See Asay, et al., Reliance Server for Electronic Transaction System for related information.

4.1.5. Market Specification

To the foregoing prior art, for purposes of this distributed rule enforcement system, the following new specification to the certificate of each participant (trader or market maker (dealer or specialist)) are added.

market specification = {

market_spec = { list or description of markets },
product_spec = { list or description of products },
trading_rights = { trader, dealer, official, etc. },
sponsoring broker = { one or more brokers }

}

For purposes of this market specification:

- "market_spec" is (a) a list of specific markets (e.g., NYSE, AMEX, NASDAQ, CHX, PSE, BSE, PHLX, MATIF, DTB, CBOE, CME, COMEX, etc., or (b) a description that may apply to many markets (e.g., "US equity markets with an average daily volume for the preceding year in excess of 1 million shares/day" or the like)

The following would be a valid market description:

market_desc = {
exchange country = US .AND.
exchange type = listed equity .AND.
average daily volume >= 1000000 shares/day .AND.
daily volume base year = current year - 1 .AND.
.NOT. exchange code = CHX, PHLX, BSE, PSE
}

- "product specification" is a list or description of specifically allowed products (e.g., stocks, bonds, listed options, OTC options, derivatives, commodity futures, etc.). It may also be specified down to the instrument level (e.g. by CUSIP number, ticker symbol, or the like), and may be specified with respect to the properties of the instrument (e.g., all issues of common stock on which Brokerage Firm X is stated to be the underwriter, dealer, market maker; or common equity of all companies having a market capitalization in excess of $2 billion).

The following would be a valid product description:

product_desc = { listed equity, listed equity options, OTC equity,
OTC equity options, commodity futures }

- "trading rights" is a list of the privileges the subject has with respect to the product group in the specified market. The rights to buy, sell, bid, ask, buy options, write options, view the pending order book, and others may be separately granted or denied with respect to a given product or class of products. An official, whether of the exchange or from a regulatory body, may also have the right to view and participate in the market. They cannot buy or sell, but can view the order book approve or disapprove a given trade, and halt trading if necessary.

  Most likely, a participant may have a certificate that allows them (a) the right to trade (take market) in many products on many markets, subject to credit and broker sponsorship, but (b) only the right to "make market" in a relatively small number of products (i.e., post bid and ask prices and sizes, and view the book of pending orders, etc.). Hence it is expected that these attributes will be grouped together to reflect these relative associations, as shown in the example below.

- "sponsoring broker" is a list of one or more brokers that stands behind (makes itself legally liable for) the trades placed by the subject by:

  countersigning the subject's trades before they are placed

  confirming the subject's trades after they are placed

A more complete and realistic example might be the following:

```
list_of_markets {
    [1] { market_spec = {
            exchange country = US        .AND.
            exchange type = equity       .AND.
            exchange average daily volume >= 1000000 shares/day }
        product_spec = ALL,
        trading_rights = buy/sell,
        sponsoring_broker = Charles Schwab },
     [2] { market_spec = CHX,
        product_spec = { GM, IBM, Raytheon }
        trading_rights = { buy/sell, bid/ask, view_book }
        sponsoring_broker = Midwest Discount }
```

}

In this example, the person holding the certificate possesses ordinary trading rights in any US equity market with an average daily volume greater than or equal to 1 million shares per day. However, in addition, on the Chicago Stock Exchange, they have the right to act as a dealer or specialist in three stocks (specified here by enumeration).

Products for which a participant has special trading rights could be identified in other ways, such as by some common property (e.g., stocks underwritten by a given dealer), or by the name of an access control (group) list (ACL) maintained within the exchange's computer system, etc.

These specifications apply mainly to market access and trading rights for purposes of placing and executing trades with unknown counterparties. For authenticating the non-trade related messages of system or market administrators, exchange officials, or overseeing regulators, it is sufficient to specify their roles, restrictions, and document types as noted above.

What is new here is the concept of specifying the allowed markets and trading rights in a participant's certificate.

Allowed markets could possibly be considered falling within the prior art concept of authorized counterparties, but there is no counterparty or definite class of counterparties specified, as would be required if the sponsor were to exercise control over the parties with whom its agent trades. To achieve that, an authorized counterparty specification will still be required.

Trading rights could be subsumed under the prior art concept of allowed roles, but the currently existing roles of trader, dealer, specialist, etc. are not specific enough to directly imply the ability to post price quotes on specific stocks or view an order book in a market system.

Alternatively, even if these specifications were regarded as obvious applications under the prior art, a novel manner of enforcing the restrictions they create is provided in the process specifications below.

In addition to product and rule specifications, the system can specify trade data formats, trade matching rules, trade routing strategies, external limits, external processing requirements, source / destination requirements, and warranties as to source / destination.

A payment / delivery specification may include:

payment_spec = { one or more bank accounts },

delivery_spec = { one or more custody accounts }

4.2. Enforcement Framework

The trading, market, product, routing, and other rules defined in this system can be enforced by any party having copies of the relevant certificates and the capacity to verify those certificates and compare them to the specifics of a given transaction.

1. By Participant. The participant himself may retrieve all relevant certificates and make his own determination as to whether a given transaction will be allowed. He may often do so, to check the current validity of any given strategy he seeks to execute. However, from a regulatory viewpoint, the participant cannot in general be trusted to enforce rules against himself, other than in an honor system.
2. By Market. The market is in a better position to validate a given transaction and enforce rules against the participants, since it can refuse to perform the transaction if it is found to violate any important constraint. It will generally do so, to avoid announcing or posting any execution, only to have it unwound later on when it is found to be in error. Also, this system assumes the emergence of numerous markets trading in innumerable products, many of which may lack solid financial or legal responsibility. Also, the market cannot be trusted to enforce rules governing its own operation, any more Therefore it is a significant objective to enforce rules against the market
3. By Clearinghouse
4. By Trusted Device in Market System

4.3. Certificate Definitions

4.3.1. Market Certificate

A market certificate is issued by a regulator to an exchange market (dealer, order-driven, etc.) to identify the market, its sponsors and rules, and specify what classes of products it may trade.

A regulator may include (a) a government agency having jurisdiction over the products in question (e.g., US Securities and Exchange Commission, US Commodity Futures Trading Commission, US Federal Energy Regulatory Commission, US Environmental Protection Agency, etc.), or (b) an industry trade association which promulgates rules concerning trading activity and may provide a dispute resolution procedure (e.g., National Assn of Securities Dealers, National Futures Assn, National Grain and Feed Assn, Electric Power Research Institute, American Petroleum Institute, etc.)

Note that the regulator may issue the certificate in its own name, or it may direct another to issue it on its behalf or under its authority. For example:

market certificate = {
identity specification = {
issuer = Chase Manhattan Bank,
serial number = 12345678,
on_behalf_of = Federal Energy Regulatory Commission,
subject = Northeastern States Electric Power Exchange,
sponsor = { Northeastern Electric Cooperative Association, Inc.
2 State Street, Boston, MA 02177 USA, 617-222-1111 },
network domain address of market = mkt.nsepe.com,
pointer to rule book = http://www.nsepe.com/pub/rules.html,
subject public key info = F1e33S58hjRdFgSjfzFbhKEfd578, etc.
valid dates = 1-1-1997 through 12-31-1998 },
product specification = {
electric power for spot delivery (within 24 cycle),
electric power forward contracts,

```
                electric power futures and options,
                pollution allowances (SO2, CO, etc.),
                electric power transmission capability,
                #8 copper wire for spot or forward delivery,
                taxes collected on generation, transmission or use },
        allowed participants = {
                spot and forward {
                        industrial buyers holding class X certification
                        municipal buyers holding class Y certification
                        power brokers holding class Z certification },
                futures and options { same + accredited investors },
                pollution allowances { same + accredited investors },
                tax collection { relevant terrestrial governments } },
        technical specification = {
                framework = CHOICE { open outcry, specialist, dealer }
                auction type = CHOICE { continuous auction, one-price auction,
                        Dutch auction, Vickrey (2nd price) auction, etc. }
                matching rules = { open rule[32], close rule[44],
                        optimization[127, 128, 133], etc. } },
                clearinghouse = State Street Energy Clearing Services, Inc.
                payment agent = State Street Bank
                payment terms = {
                        principal participants = monthly net settlement,
                        accredited investors = T+3 }  -- i.e., 3 days after trade }
        issuer signature = R2e3Yg5f7J9nD-d7Y5k3J6R7l8S9fTg...
}
```

Such a certificate identifies the market, its sponsoring organization, the products it is allowed to trade, and the participants allowed to trade them, and certifies a public digital

signature key, which it can use to authenticate itself. It might also specify the types of optimization and matching rules to be used, as will be described later.

While such a certificate might seem unnecessary for large existing exchange market systems, this distributed rule enforcement system can allow proliferation of tens of thousands or millions of separate exchange markets, operating on a worldwide basis. In that context, it will be vitally necessary for such information to be readily known to all participants and certified by an appropriate terrestrial regulatory entity.

Note that this market certificate contains the notion of "use-conditions," such as the qualifications required of participants, the products they can trade, settlement and payment terms, etc. This amounts to a joint statement by the market authorities and the issuing regulatory entity, specifying who may use the market and what rights they have.

As shown in the drawings:

Market Certificate = {
M1 Identity / Reliance
M2 Market Desc. Info
M3 Product Spec.
M4 Participant Spec.
M5 Trade / Match Rules
Regulatory CA Signature }

4.3.2. Product Certificate

A product certificate is issued by a regulator and applies to a specific product's textual and data description (data format, rule set, and terms & conditions) specifying how it may be traded in an approved manner, who may modify it, etc.

product certificate = {
identity specification = {
name = spot electricity for delivery within 24 hours
sponsor = EPRI,

product data format = {
pointer = www.epri.org/prod/spot_elec.cgi,
hash = k1E4Ft7jU8hO0aH5nF4fS3jGhn }
terms and conditions = {
pointer = www.epri.org/terms/spot_elec.html
hash = k1E4Ft7jU8hO0aH5nF4fS3jGhn }
standard contract units = MKWH (million KWH)
standard contract size = 10
market specification = {
list or types of markets on which this product may trade }
match rule specification = {
open rule = { allowed market opening rule(s) },
close rule = { allowed market closing rule(s) },
match rule = { allowed trade matching rule(s) } }
trading rules = {
max bid-ask spread = { 2% of current price }
participant specification = {
ordinary = { requirements to buy/sell this product },
dealer = { requirements to post bid/ask prices for product },
market maker = { requirements to view the order book, if any } }
}

As shown in the drawings:

Product Certificate = {
P1 Identity / Reliance
P2 Product Desc. Info
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
Regulatory CA Signature }

4.3.3. Rule Certificate

A rule certificate is a certificate issued by a regulator which applies to a specific trade matching rule, including its textual and data description (pseudo-code, executable code, and terms & conditions) specifying how it may be applied in an approved manner, who may modify it, etc.

As shown in the drawings:

Trade / Match Rule Certificate = {
R1 Identity / Reliance
R2 T/M Rule Desc Info
R3 Product Spec.
R4 Market Spec.
R5 Participant Spec.
Regulatory CA Signature }

4.3.4. Participant Certificate

A participant certificate may be issued by any reputable CA, such as a bank, under authority from a regulator or market, attesting to the identity and qualifications of an individual user to participate in allowed trading markets, handling allowed products, under allowed trading and matching rules. Allowed markets, products, rights, and trading/matching rules may be grouped in different ways, either by the use of parenthesis and macros within the same certificate, or more likely by the use of different participant certificates for each principal combination of rights.

As shown in the drawings:

Participant Certificate = {
U1 Identity / Reliance
U2 Authority Spec
U3 Market Specs {
U4 Allowed Products,

U5 Allowed T/M Rules,

U6 Trading Rights }

Bank CA Signature }

4.3.5. Index Certificate

An index certificate is a certificate issued by a regulator or market which codifies and fixes the definition, formulas, and rules (terms and conditions) for a market index. As the index composition, formulas, and/or terms and conditions change over time, new certificates will be issued for each such version. Old versions may remain outstanding as they continue to certify the composition of the index for historical purposes, even after they have been superseded by a newer index definition.

As shown in the drawings:

Market Index Certificate = {

R1 Identities / Reliance

R2 Market Index Spec. = {

R3 Components

R4 Calculation Method

R5 Version Number }

Registering CA Signature }

5. Recap of Rule Enforcement Data Formats

5.1. User Transaction = {

T1 To: Market ID

T2 From: Participant ID

T3 Transaction ID

T4 Action Type (Buy, Sell, etc.)

T5 Product Spec.

T6 Trade / Match Rules

T7 Satisfaction .Function (P,Q, etc.)

Participant Signature }

5.2. Execution Report = {
E1 To: Clearinghouse ID
E2 From: Market ID
E3 Participant ID Data
E4 Transaction ID Data
E5 Broker/Dealer IDs
E6 Product Spec.
E7 Trade / Match Rules
E8 Deal Terms (P,Q, etc.)
E9 Transaction Context
E10 User Trans. Digests
Market Signature }

5.3. Market Certificate = {
M1 Identity / Reliance
M2 Market Description
M3 Product Spec.
M4 Participant Spec.
M5 Trade / Match Rules
Regulatory CA Signature }

5.4. Participant Certificate = {
U1 Identity / Reliance
U2 Authority Spec
U3 Market Specs {
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights }

Bank CA Signature }

5.5. Product Certificate = {
P1 Identity / Reliance
P2 Product Desc Spec.
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
Regulatory CA Signature }

5.6. Trade / Match Rule Certificate = {
R1 Identity / Reliance
R2 T/M Rule Desc Info
R3 Product Spec.
R4 Market Spec.
R5 Participant Spec.
Regulatory CA Signature }

5.7. Market Index Certificate = {
R1 Identities / Reliance
R2 Market Index Spec. {
R3 Components
R4 Calculation Method
R5 Version Number }
Registering CA Signature }

6. Secure Distributed Accounting System: Overview

There is a general need to securely administer business, governmental, or organizational (generally "administrative") functions, inter alia to prevent fraud, assure compliance with stated rules (both before and after an action is taken), divide approval

processes in accord with sound principles of government, and provide a secure record of actions taken. Such secure administration can help to reduce fraud and corruption, facilitate selective sharing of information, insure compliance with rational rules and procedures, and generally enhance the audit and administrative processes, thereby enhancing the accountability and credibility of business and political institutions.

In many parts of the world, it is difficult to foster social or economic development by investing in private enterprises or providing foreign aid, due to likelihood that (a) funds will be misapplied and diverted to the private use of individuals (e.g., flight capital, which often winds up back in Swiss or US banks), or (b) data regarding an enterprise's sales, costs, profits, losses, assets, inventory, and other normal bookkeeping information, which (under US accounting rules) should be reported to investors on a regular basis, will be unavailable, unacceptably delayed, or falsified, due to lax reporting requirements and business practices in the host nation.

In some cases a nation's court system may refuse to provide legal remedies in accord with the rule of law, or may be incapable of enforcing its laws against bribery, corruption, organized crime, etc. In such cases, an effective transactional oversight capability, hosted securely in a different country that does support the rule of law, can provide a framework for securely and properly administering an investment that may help minimize or avert losses to the outside investors.

The present invention provides a (a) general oversight framework by which the internal financial and accounting controls, as well as other rule-governed activities of a subject entity, can be greatly strengthened, and (b) elucidates a wide range of specific examples in which the oversight framework can be applied to produce useful results.

Several general methodologies are employed in this system:

1. Dual Control. The public key digital signature of an entity or its officers can be based on a private key that is split into two or more fragments, with one held by the nominal signer (subject) entity and the other(s) held by a confirming (or oversight) entity. The signer's digital public key certificate, issued by a CA as described herein, may contain an indication that one or more oversight entities is involved, which can be either named or anonymous.

2. Co-Signatures. Alternatively, the subject entity/signer's digital public key certificate can specify a required co-signer [as in Fischer] or state that there is a confirmation requirement [as in Sudia]. In this case the named required co-signer or confirmer can be the oversight entity.
3. Most likely the oversight entity would be a bank, CPA firm, or some other well recognized entity trusted to enforce the rules as described herein. In some cases it might be a government agency or administrative control board (e.g., a State Department of Finance), or it could be a parent corporation, major investor, superior government (e.g., cabinet) department, or another entity with "parental" responsibility toward the subject.
4. There is no technical limit on the number of oversight entities that could be employed for a given subject entity/signer, but given the detailed procedures to be followed by each one, there may be operational cost and liability exposure barriers that will make it preferable to limit the number of oversight entities to at most 2-3 per subject, and in most cases one should be enough. Also, when more entities are involved, there will be performance barriers such as excessively long response times (should stay under a few seconds) and arduous database recovery and synchronization requirements in the event of faults or errors.
5. Database and Rules. Once there is a defined oversight relation for a given set of official actions, the overseeing party may maintain either (a) a complete (mirror) copy of the entire financial and administrative bookkeeping system of the subject entity, (b) a summary of information relevant to the overseer's decisions, (d) such information as is needed to operate the system of rules the overseer is required to enforce, or (d) possibly a complementary set of data (such as a partial ledger) that is related to but not identical to the ledger components maintained by the subject.
6. CA Certificates. Under this system a CA issues a certificate that creates the oversight relationship. Typically, the CA is knowledgeable of this control system and is an active participant in helping to create and enforce the relationships defined herein. This certificate can be for a single public key that is partially held by the oversight entity, or for a key that is entirely held by the subject, but there is a stated co-signer or

confirm-to requirement. When a recipient gets a signed document or transaction from the subject, they know in the first case the overseer must have contributed to the signature, or in the latter, the overseer's separate digital signature and associated public key certificate is also required to be present.

7. End-User Contracting. It is possible to require the recipient to verify an arbitrary set of conditions that may be expressed in the certificate or in the signature itself, prior to becoming entitled to rely on the transaction or seek any recovery against the parties thereto, and to be legally bound by such terms and conditions, including limitations on liability and venue for seeking remedies for perceived losses or wrongs. One example of such an "end-user contracting" methodology is described in Sudia, 3-24-97.

8. Traceable Payments. Building on the aforementioned end-user contracting capability, it is possible to define payment means that remain traceable through any number of transfers to aid in identifying improper transfers, diversions, and laundering of funds. Such traceable payment accounts constitute a further element of this system of financial controls.

7. Summary of Secure Distributed Accounting

A subject entity receives a public key certificate which contains the condition (either explicit or implicit) that its signature is not valid without the consent of an oversight entity. The subject signs a business transaction in the ordinary course of business and sends it to a recipient, along with the subject's certificate, and the recipient validates the signature and the certificate, including verifying any conditions that may be stated in the certificate.

Prior to becoming valid, the transaction is first sent to the oversight entity, which may merely record it in a mirrored database for audit purposes, or it may check the transaction against some number of pre-determined rules to determine if it is valid according to those rules, confirming if it is okay, and declining to confirm and issuing an error message if it is not.

As shown in **FIG 6**, a subject entity receives a digital public key certificate [1] from a CA, where the subject's signature is not complete or valid unless partially signed,

co-signed, or confirmed by an oversight entity. Where relevant the overseer also receives a digital public key certificate [2].

The subject entity normally maintains a database or ledger detailing each business transaction as well as maintaining cumulative running totals for various important financial values and ratios, and checking the transaction against its internal business rules prior to issuing it.

However, for many reasons, the subject entity might not be trusted to make its decisions and keep its records in an entirely competent or honest manner. Hence, under this system the transaction is required to be sent to the oversight entity for partial signature, co-signature, or confirmation.

The oversight entity also maintains a database, which may be a full (mirrored) copy of the subject's database, or a subset or complement thereof, or may be a set of running totals with a series of rules to be applied in various cases.

The computer systems of both subject and overseer are programmed to process a set of pre-determined transactions. Also, there is a class of maintenance transactions that may be initiated by either party to create a new transaction type, decision rule or account type, modify an existing one, or delete an old one, typically taking effect only upon consent of the immediate overseer or some other overseer made responsible for approving such changes.

The subject entity forms and signs (or partially signs) a business transaction [3], updates its own database, and sends it to the overseer for partial signature, co-signature, or confirmation. The overseer checks the transaction, updates its own database, approves the transaction by partially signing, co-signing, or confirming it, and then either (a) sends it back [4] to the subject which passes it on [5] to the intended recipient, or (b) sends it [6] to said recipient directly.

When digitally signed and confirmed transactions are employed, there is no security concern when the controlled subject assists in sending the message back to the final recipient, because it cannot alter such a message in any case. Thus the decision to have the overseer send the transaction directly [6] might be undertaken as a matter of convenience, speed, or efficiency, or because the overseer was somehow involved in

collecting pieces of a larger transaction, but not because of any concern that the subject might alter the message.

8. Multi-Party Approval Modes (Prior Art)

FIGS 7-9 show three prior art frameworks for multiple-signature approval. Any of the three can work equally well in the present invention, along with any others which may be discovered in the future that can perform a similar function of distributing an approval function among a plurality of entities. This material is being covered here in some detail to simplify the main discussion of oversight control mechanisms that follows.

8.1. Multi-Signatures

In **FIG 7**, a subject entity [1] prepares and partially signs a document or transaction using a partial private key [k^{-1}] and transmits it [2] to the oversight entity [3] which (after performing the checks described in this invention) also partially signs it with its matched portion [k^{-2}] of the private key [K], which is then forwarded to the final recipient. The recipient receives or obtains a digital public key certificate [5] naming the Subject, and listing its public key K. Recipient already possesses the public key [6] of the CA, which it received via a trusted delivery method. It uses the CA's public key [6] to verify [7] the Subject's certificate, and then uses the Subject's public key listed therein to verify [8] the document or transaction. Note that there is only one signature and certificate, although the existence of the separate Oversight Entity should be disclosed in the certificate [5].

This process of computing multi-signatures using fragments of a private key matched with a certified public key, and many of its variants, are extensively described in US 5,825,880 and US 5, 867,578, and numerous references cited in those cases.

In a preferred embodiment, the document to be signed would be routed via a Workflow Engine to both the Subject and the Overseer, and their partial signatures would each be computed separately, in parallel. Then the workflow engine would route the partially signed documents to a "Combiner" that combines the two (or more) partial signatures into one full signature, whereupon the Workflow Engine sends the fully signed document to its intended destinations, generally sending fully signed copies to all three parties.

8.2. Required Co-Signer

FIG 8 shows a simplified overview of a required co-signer scheme, in which a Subject Entity [1] prepares and fully signs a document or transaction [2], with the proviso that its CA certificate (or secondary authority certificate) [5] states that the Subject's signature is not valid without the co-signature of the Oversight Entity, or at least is not valid by itself for certain types of transactions, such as those with a stated value of over $10. The transaction is sent to the Oversight Entity [3] for its review and approval, and after performing the checks and operations described in this invention, it will generally approve the transaction by co-signing it, and forwarding it to the Final Recipient [8]. The Recipient [8] has already received the public key [K^{+CA}] of the CA, which it received via a trusted delivery method. It obtains the certificates [5, 6] of the Subject and Oversight entities, either with the transaction or by retrieving them from a directory, verifies them using the CA public key, and in turn uses the respective public keys of the entities listed therein to verify [7] the Subject signature and Overseer co-signature, whereupon, if all signatures verify and all conditions are satisfied, it accepts [8] the transaction.

In a preferred embodiment, the document or transaction is formatted according to "PKCS #7: Cryptographic Message Syntax Standard" (or its successor, "S/MIME") and each successive signature is attached using a series of PKCS #7 signature blocks, which blocks may if desired carry the signer's certificates as unauthenticated attributes.

8.3. Required Confirmer

FIG 9 shows a third framework for requiring the Oversight Entity's consent before the Final Recipient can be permitted to legally rely on the transaction. Here the Subject Entity [1] prepares and sends a document or transaction [2] directly to the Final Recipient [3], who again possesses the public key [K^{+CA}] of the CA, which it received via a trusted delivery method.

The Recipient obtains the Subject's certificate [6], either with the transaction [2] or by retrieval from a directory, and notes that it contains an "Overseer Must Confirm" requirement and names a specific overseer (or a determinable class of overseers). The recipient then sends at least part of the transaction to Oversight Entity [4], which after performing the checks and operations described in this invention, will generally approve

the transaction by co-signing it, and return it to the Recipient [5]. The Recipient [3] obtains the certificates [6, 7] of the Subject and Oversight entities, verifies them using the CA public key, and uses the respective public keys of the entities listed therein to verify [8] the Subject signature and Overseer co-signature. If all signatures verify and all conditions are satisfied, it accepts the transaction.

The concept of a certificate attribute requiring that another must confirm a transaction before it can be considered valid for purposes of legal reliance is disclosed in Sudia et al, WO 96/02993 "Method for Securely Using Digital Signatures in a Cryptographic System."

The concept of a confirmation server, also called a "Reliance Manager," is disclosed in Asay et al, "Reliance Server for Electronic Transaction System," US 5,903,882. Please refer to Part 2 of the Asay et al specification, authored by Sudia.

8.4. Leakage of Contracting Authority

It should be noted that the technical mechanisms disclosed here for making the approval of business transactions and payment instructions of a subject entity conditional upon the assent of an oversight entity may not be entirely effective, from a legal standpoint, in preventing the subject entity from entering into enforceable contracts with third parties. Under the Law of Contracts, it is unnecessary to have a digitally signed writing, or even a writing at all, for the subject entity to become legally bound.

During meetings or telephone calls, an officer or agent of the subject entity can make an oral contract. Or a judge may find that an exchange of electronic e-mail messages has created a contract. When the contract is reduced to electronic form and authenticated (with a certified digital signature), the agent or counterparty may notice (from facts noted in the agent's or entity's certificate) that the agent did not possess valid authority or consent to make that contract (or authorize that instruction). However, the counterparty, relying upon the legal doctrines of apparent authority or implied authority, can claim that the principal (the subject entity) is legally bound by its agent's representations, especially if the counterparty changed position (e.g., shipped goods) in reliance upon the existence of a contract.

This may be termed "leakage," and it is a legal problem, whose solution lies outside the scope of the present invention. Possible countermeasures include (a) counter claim for mistake of fact, (b) legislation, or (c) creation of a novel corporate charter for "subject entities," possibly attended with a new type of chartered entity designation (distinct from existing designations such as Corp, Inc, LLC, LTD, and so on), to place all potential counterparties on legally effective notice that "leakage" contracts will not be enforced.

Sudia et al, Electronic Cryptographic Packaging, US 5,995,625, discloses mechanisms for securing the legal assent of an unknown third party to a set of system rules governing the use of a cryptographic certificate, or any other digital product capable of cryptographic wrapping. However, the recipient's assent to such system rules can only occur after he has received and attempted to use a wrapped certificate or other wrapped digital product. This works well to limit the liability and define the rights of a digital public key certificate issuer, or a seller of digital goods, but may be ineffective to prevent formation of contracts by oral or unauthenticated e-mails.

9. Multiple Entity Variations

Although there is no great effect on the main inventive concept of the present invention, it must be further disclosed that (a) there can be multiple instances of the same Subject and Oversight Entities, which would occur mainly for system reliability and recovery purposes, (b) the Oversight function can be divided among several distinct entities, under the control of different legal organizations, which may exist mainly as backups to each other for reliability purposes, or may substantively divide up roles and perform different parts of the approval process, each contributing to the resulting signature(s) and (c) the Subject entity may in fact consist of multiple entities, with varying relationships to each other, such as a corporation or government agency and its subdivisions.

As a further variation, when either the Subject or Oversight Entity is plural, the manner of computing or forming the signatures from each entity to effect complete approval can, in any given case, be based on all parties adhering to one of the three major multi-party approval frameworks given above, or as it will be obvious to one skilled in the

art, the approval of any given participating entity can be obtained and verified using any of the above or similar methods, independently of the method used by any other participant, and furthermore, one entity's approval in a given case could be expressed using any of these or similar methods, without regard to how approval was expressed by that same entity in any prior approval. That is, one conceivably could arbitrarily switch between any of the methods on any given transaction, although most likely such switches would occur only in accord with pre-determined procedures to be followed, e.g., for different types of transactions, or for transactions with different types or classes of Final Recipient, etc.

FIG 10 shows a simple but desirable multi-entity configuration, in which there are still only two legally distinct entities, the Subject Entity and the Oversight Entity, but both of them are mirrored replica sites for reliability and disaster protection, thereby giving the effect of four separate entities (since it is undesirable to mirror a private key fragment). The multi-signature group signs with a single key which here has been divided into four fragments [k^{-1}... k^{-4}], of which any two are sufficient to form the valid signature of the Subject Entity (i.e., a "2-of-4" multi-signature scheme) as taught by and Brickell et al and references cited therein. In accordance with the present invention, approval by the Oversight entity is conditional on its first performing a pre-determined set of checks and other operations, as further described below.

As shown in **FIG 10**, a Subject Entity forms a document or transaction, partially signs it with its private key fragment [k^{-1}], and forwards [1] the partially signed transaction to a Combiner [4] (as further described in Brickell et al). At the same time, it forwards a copy [2] of that transaction to the Oversight Entity, which after performing pre-determined checks and other operations, typically approves and partially signs its copy with its private key fragment [k^{-3}] and forwards [3] the second partially signed result to the Combiner [4]. Upon receiving the second partially signed transaction [3], the Combiner [4] combines the two partial signatures to form one whole signature, which it then appends to the transaction, discards the partial signatures, and sends the result [5] to the Final Recipient.

The operation of combining two or more partial signatures to form a full one does not require high security, because knowledge of the partial signatures does not allow an

attacker to compromise the approval process. Therefore the act of combining such partial signatures could just as well be performed on a desktop, or by the Final Recipient. However, because it is a tedious chore, a Combiner is provided within a workflow system to automate the task. After the Combiner has done its work, it will typically discard the two partial signatures, which were already journalized by the signers, which as shown above are both mirrored, so all data stored at the primary site (except for the private signing key) is replicated in real time. This allows the Combiner to be simple, fast, and light.

In case the primary Oversight Entity site becomes unavailable, due to a system or network or other failure, the Oversight Entity "cuts over" to its mirror site, and in accord with well known principles of reliable computing system design and operation, it typically notifies the Subject Entity (which here is still operating normally) to send transactions [7] to its mirror site. At the mirror site the Oversight Entity performs the same pre-determined checks and operations (or similar ones) prior to approval as it would have performed at its primary site, partially signs the transaction, and sends the result [8] to the Combiner [4], which combines the partially signed transactions into one fully signed one and forwards [5] that to the Final Recipient, which verifies the transaction using the Subject's digital public key certificate and the public key [K^{+CA}] of the CA, which it received via a trusted delivery method, and accepts or rejects the transaction [6] based on the outcome of said verification.

A further variation will exist where the Oversight Entity does not solely approve or reject a transaction proposed by the Subject Entity, but itself is a substantive participant in determining the content of the transaction. Such a configuration could exist where two or more Subject Entities were both involved in planning and executing the transaction, and at least one is serving as an Oversight Entity for the other.

Whenever the second entity must contribute data to the same signed transaction, then the multi-signature method may become impractical, as the partial signature of the first entity becomes invalid if the second entity adds or changes the transaction data. However, such a process can be supported via the required co-signer or required confirmer frameworks. Under either of those frameworks, it would not be unusual for the Oversight

Entity, in addition to approving the Subject Entity transaction, to furnish some additional data, such a transaction approval sequence number, or any other data that might be useful for the Final Recipient.

For example, according to the present invention, if a parental Cabinet Department (CD) were serving as the oversight entity for a specific Bureau (B) of a Government, then CD could confirm B's financial transactions, adding to them such useful information as the CD level account number from which the funds will be derived, and specifying in real time a bank account number from which the funds can be drawn. In another example, a parent insurance company may exercise oversight authority over all transactions of a local insurance subsidiary, and in addition to approving each policy written or claim paid, the parent (in addition to administering a set of solvency and diversification rules, as further discussed below) can also furnish in real time a master binder number for a policy or a bank account number from which a payment is to be made.

It will be appreciated by one skilled in the art that (1) the foregoing approval frameworks and reliable computing topologies can be combined with each other to produce many obvious variations thereof, and that (2) the underlying business transactions themselves can be designed to be carried out in a step-wise fashion, with oversight approval attaching to a transaction received from a prior step, and new information being contributed toward a future step. In some embodiments, a transaction formed by one entity is approved by an oversight entity that adds some new data, and the result is subject to oversight by yet another oversight entity which checks either (a) the new material added in step 2, or (b) the entire transaction as formed by both steps 1 and 2, and so on. This process could continue through many steps, each of which may have an oversight approval requirement, and some data from previous steps may be forwarded, together with evidence of prior oversight, through an indeterminate and possibly lengthy series of such operations.

10. Oversight Startup and Maintenance

It is an objective of this system to provide a form of electronically administered power, authority, or discretion to an entity, such as a certified digital signature capability and/or access to designated bank accounts or other digitally managed rights, but to make that access conditional on the (usually contemporaneous) approval of an oversight entity,

where said oversight entity's approval is manifested by, for example, its jointly signing, co-signing, or confirming the transaction proposed by the subject entity, and doing so according to a predetermined set of tests and/or other operations, which are to the greatest extent possible, fully automated to support straight through processing.

Accordingly, it is necessary to initialize the state of such a system so that the databases and transaction rules for the subject entity and oversight entity are initially synchronized, remain synchronized throughout the operation of this system, are capable of being modified and updated to accommodate new pre-agreed rules and procedures that may be duly adopted by the parties, and to recover gracefully and correctly from any processing errors that may occur, whether due to mechanical failures, software defects, or other human errors.

The following sections explain how the oversight architecture would be initialized, maintained, and terminated. These concepts are generally applicable to all forms of oversight systems contemplated in this invention, without regard to the specific rules and data structures involved in each.

10.1. Example: A Simple Accounting System

To facilitate this discussion of system startup, operation, and maintenance, consider the following example.

In one embodiment, this system can be used to implement a set of rule based controls around an accounting system, typically for the benefit of a lender or investor. The objective would be to assure via the oversight entity that 2 general rules are followed:

a. The accounting system's "books" always remain in balance, and
b. No payment orders are authorized against a given bank account unless sufficient funds are available in it.

10.2. Oversight Plan

As a first step, the subject entity [company] and oversight entity, possibly in cooperation with (a) the lender or investor [PAA: plan approving authority], and (b) the bank that holds the account [DTI: deposit and transfer institution], would develop and agree to an oversight plan, to be implemented and followed in all relevant transactions.

The oversight entity could be the PAA or DTI, or any other specialized entity holding itself out as a provider of secure distributed business oversight services.

In addition the plan would specify the precise mechanism of the control structure, and identify the certification authority that will issue a certificate for the subject's signature, conditional upon the oversight process. This certificate would be come active upon completion and verification of all processes needed to assure that the oversight model is implemented and is operating correctly.

10.3. Oversight Model and Initial Rules

Under such an oversight model, the subject and oversight entities would agree upon an approved accounting method and chart of accounts, and a pre-determined set of transaction types and formats that could be initiated by the subject entity and forwarded to the oversight entity for approval.

The process can be further defined to include issuance of certificates, initial state data input and approval, change data (add, modify, delete), migration to new oversight model, and oversight termination and wrap-up.

11. Useful Rule Enforcement Paradigms

The secure distributed accounting system can enforce a variety of rules or conditions:

Simple mirrored database (keep a true copy), double entry with credit debit separation, bank risk capital rules, payment processor R > T constraint, insurance capital rules and monitoring.

Creation of business corporation or subsidiary: pre-input of approved corporate directors, name reservation with [Delaware] secretary of state, selection and instantiation of capital structure, registration with [Delaware] secretary of state, asset transfers, stock issuance, appointment of initial board and officers, creation of action and contracts register.

Governmental procedures: instantiation of constitution, organic act, or charter; unicameral legislature; bi-cameral legislature with differing terms of office; executive signing or veto requiring super majority; parliament that elects the prime minister.

Administration of statutes, regulations, or case law; according to law; according to analogous reasoning; constitutionality of law.

Due process: preliminary notices, event driven notices, opportunity to present evidence, rights of appeal.

Personnel manning charts: anti nepotism. Counterparty approvals: anti conflict of interest. Warranty services.

It is noted that the foregoing examples have been provided merely for the purpose of explanation and are in no way to be construed as limiting of the present invention. While the present invention has been described with reference to certain embodiments, it is understood that the words which have been used herein are words of description and illustration, rather than words of limitation. Changes may be made, within the purview of the appended claims, as presently stated and as amended, without departing from the scope and spirit of the present invention in its aspects. Although the present invention has been described herein with reference to particular means, materials and embodiments, the present invention is not intended to be limited to the particulars disclosed herein; rather, the present invention extends to all functionally equivalent structures, methods and uses, such as are within the scope of the appended claims.

What is claimed is:

1. A method of processing a transaction for the purchase or sale of a financial instrument wherein, one or more parties agree upon a price using an exchange market trade matching system, each party signifies their agreement by digitally signing a version of the transaction using a private key, the exchange market trade matching system confirms that the said transaction was agreed to using its facilities by digitally signing a version of the transaction using a private key, said exchange then passes all components of the transaction to a clearinghouse, said clearinghouse compares said transaction and its components with the specifications contained a market specification certificate, issued by a market regulator, to determine if the transaction was permissible for the said market, and accepts or rejects the transaction for processing based on the results of said comparison.

2. A method of approving an electronic transaction wherein, a subject entity (a) approves a financial transaction, (b) makes an entry into its subject accounting database, (c) creates an electronic transaction to effect such financial transaction, (d) digitally signs it using a private key, and (e) transmits the said electronic transaction to an oversight entity, (f) the oversight entity receives the said electronic transaction and verifies the origin and digital signature thereon, (g) checks for any applicable rules or limits that might be violated by the proposed transaction, (h) makes a corresponding entry into its oversight accounting database, and (i) completes the digital signing process using a private key, where the subject entity's signature is not valid to effect the financial transaction without such completion.

FIGURE 1.

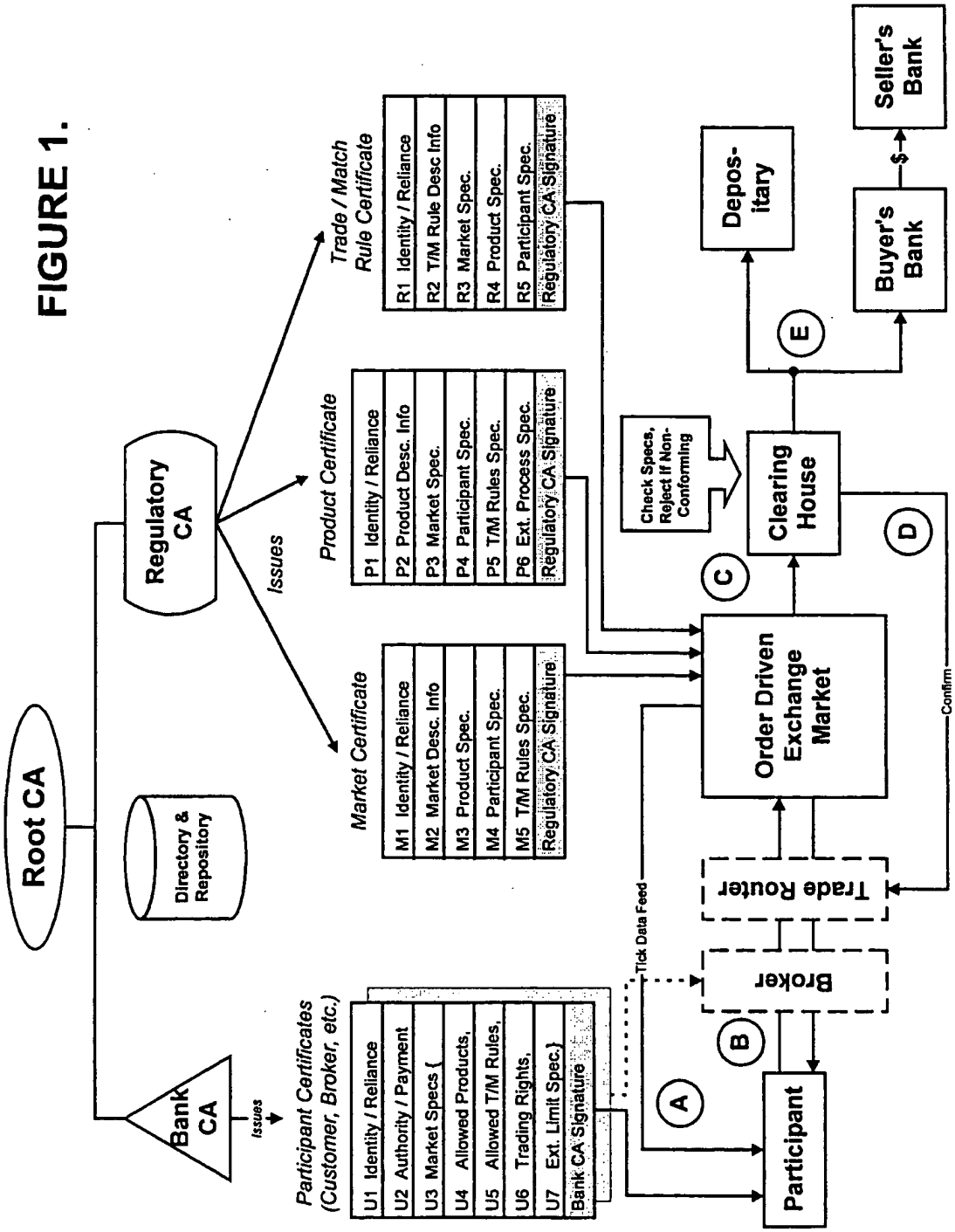

Root CA
Directory & Repository
Regulatory CA
Issues
Bank CA
Issues
Participant Certificates (Customer, Broker, etc.)
U1 Identity / Reliance
U2 Authority / Payment
U3 Market Specs (
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights,
U7 Ext. Limit Spec.)
Bank CA Signature
Market Certificate
M1 Identity / Reliance
M2 Market Desc. Info
M3 Product Spec.
M4 Participant Spec.
M5 T/M Rules Spec.
Regulatory CA Signature
Product Certificate
P1 Identity / Reliance
P2 Product Desc. Info
P3 Market Spec.
P4 Participant Spec.
P5 T/M Rules Spec.
P6 Ext. Process Spec.
Regulatory CA Signature
Trade / Match Rule Certificate
R1 Identity / Reliance
R2 T/M Rule Desc Info
R3 Market Spec.
R4 Product Spec.
R5 Participant Spec.
Regulatory CA Signature
Check Specs, Reject If Non-Conforming
Clearing House
Depos-itary
Buyer's Bank
$
Seller's Bank
Order Driven Exchange Market
Trade Router
Broker
Participant
Tick Data Feed
Confirm
A
B
C
D
E

FIGURE 2.

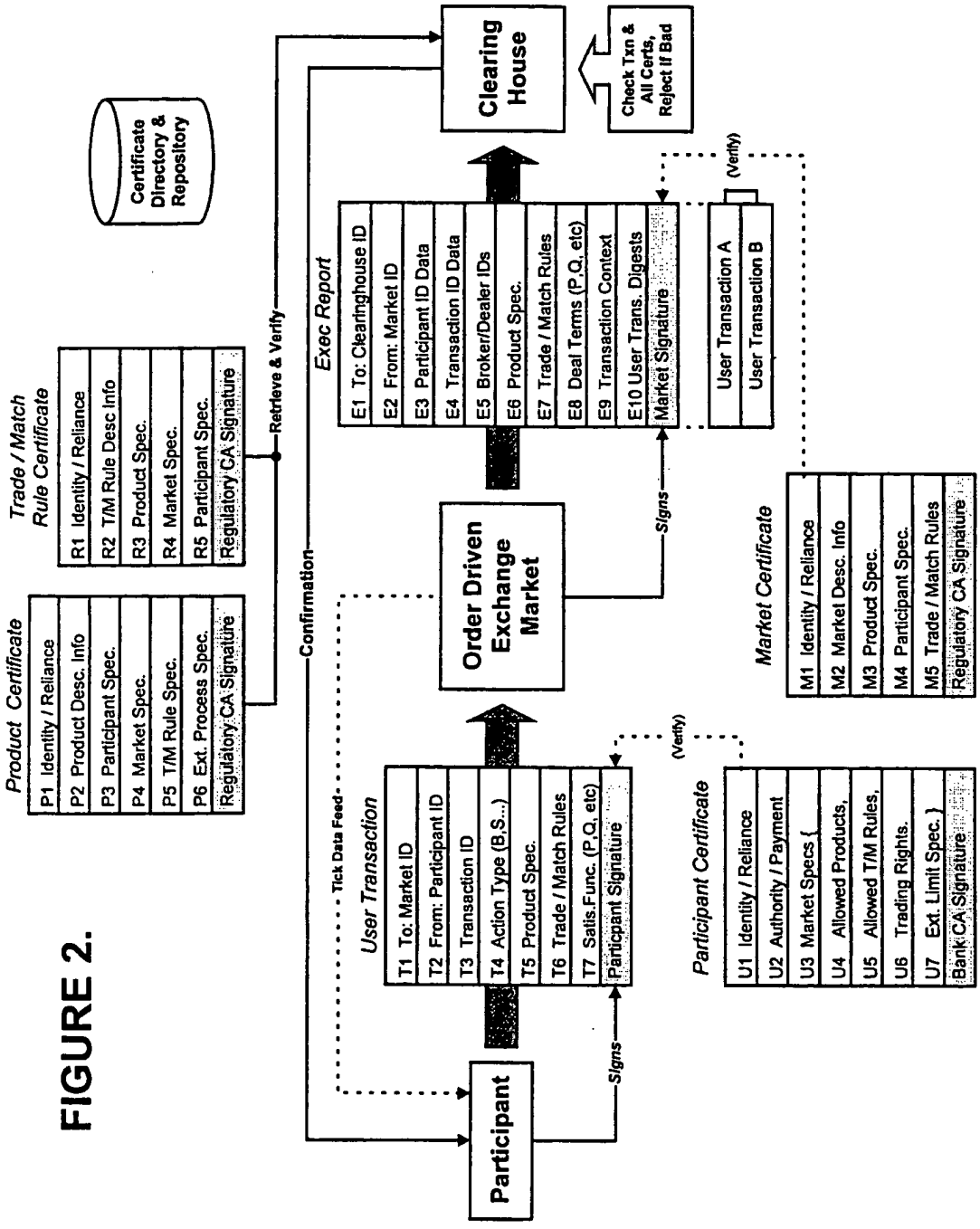

Product Certificate
P1 Identity / Reliance
P2 Product Desc. Info
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
P6 Ext. Process Spec.
Regulatory CA Signature
Trade / Match Rule Certificate
R1 Identity / Reliance
R2 T/M Rule Desc Info
R3 Product Spec.
R4 Market Spec.
R5 Participant Spec.
Regulatory CA Signature
Certificate Directory & Repository
Retrieve & Verify
Clearing House
Check Txn & All Certs, Reject If Bad
Exec Report
E1 To: Clearinghouse ID
E2 From: Market ID
E3 Participant ID Data
E4 Transaction ID Data
E5 Broker/Dealer IDs
E6 Product Spec.
E7 Trade / Match Rules
E8 Deal Terms (P,Q, etc)
E9 Transaction Context
E10 User Trans. Digests
Market Signature
User Transaction A
User Transaction B
(Verify)
Confirmation
Tick Data Feed
Order Driven Exchange Market
Signs
User Transaction
T1 To: Market ID
T2 From: Participant ID
T3 Transaction ID
T4 Action Type (B,S...)
T5 Product Spec.
T6 Trade / Match Rules
T7 Satis.Func. (P,Q, etc)
Participant Signature
Participant
Signs
(Verify)
Participant Certificate
U1 Identity / Reliance
U2 Authority / Payment
U3 Market Specs (
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights.
U7 Ext. Limit Spec.)
Bank CA Signature
Market Certificate
M1 Identity / Reliance
M2 Market Desc. Info
M3 Product Spec.
M4 Participant Spec.
M5 Trade / Match Rules
Regulatory CA Signature

FIGURE 3.

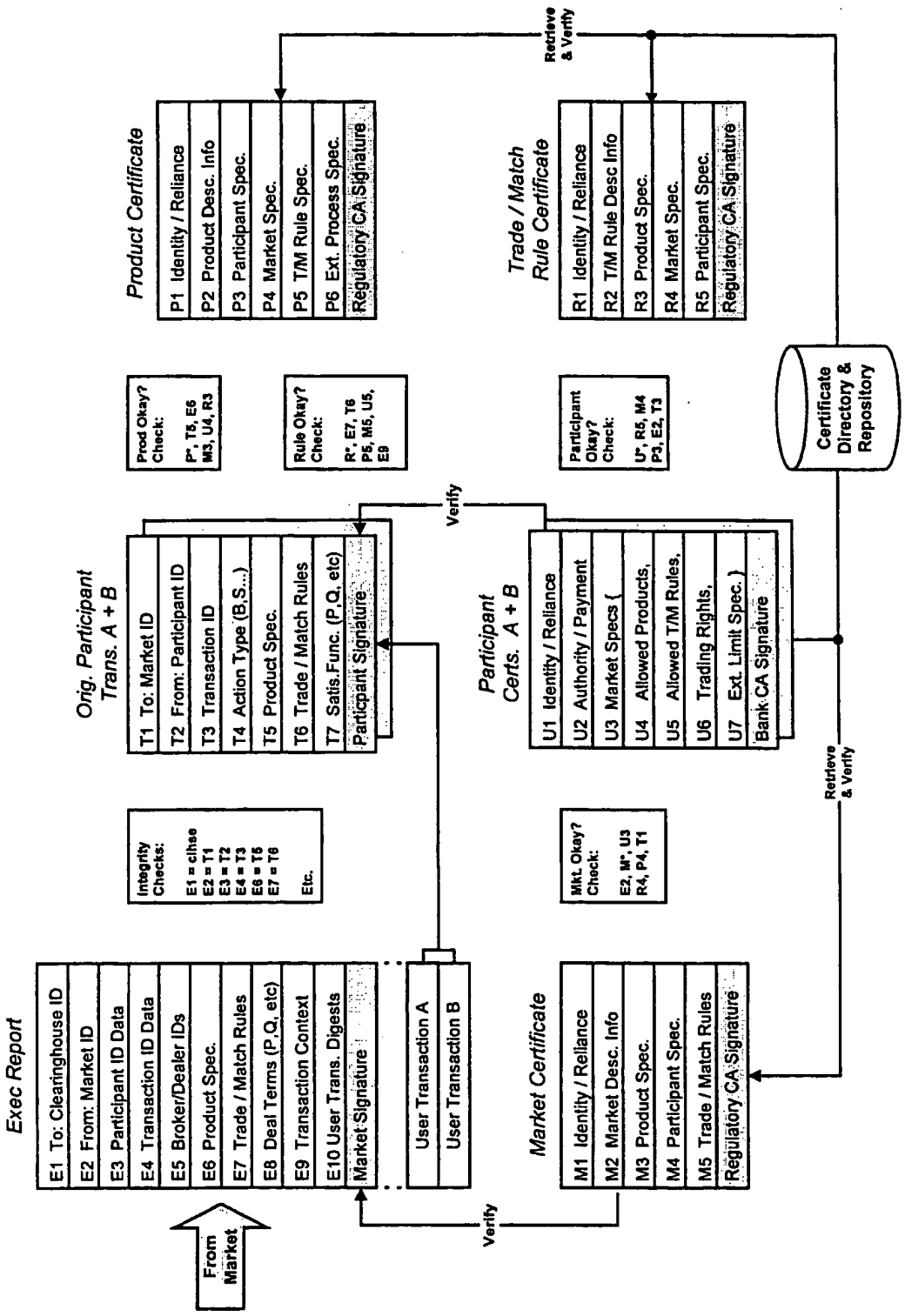

Exec Report
E1 To: Clearinghouse ID
E2 From: Market ID
E3 Participant ID Data
E4 Transaction ID Data
E5 Broker/Dealer IDs
E6 Product Spec.
E7 Trade / Match Rules
E8 Deal Terms (P,Q, etc)
E9 Transaction Context
E10 User Trans. Digests
Market Signature
From Market
Integrity Checks:
E1 = clrhse
E2 = T1
E3 = T2
E4 = T3
E5 = T5
E6 = T6
E7 = T8
Etc.
Orig. Participant Trans. A + B
T1 To: Market ID
T2 From: Participant ID
T3 Transaction ID
T4 Action Type (B,S...)
T5 Product Spec.
T6 Trade / Match Rules
T7 Satis.Func. (P,Q, etc)
Particpant Signature
User Transaction A
User Transaction B
Verify
Product Certificate
P1 Identity / Reliance
P2 Product Desc. Info
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
P6 Ext. Process Spec.
Regulatory CA Signature
Prod Okay? Check:
P*, T5, E6 M3, U4, R3
Rule Okay? Check:
R*, E7, T6 P5, M5, U5, E9
Trade / Match Rule Certificate
R1 Identity / Reliance
R2 T/M Rule Desc Info
R3 Product Spec.
R4 Market Spec.
R5 Participant Spec.
Regulatory CA Signature
Retrieve & Verify
Participant Okay? Check:
U*, R5, M4 P3, E2, T3
Certificate Directory & Repository
Participant Certs. A + B
U1 Identity / Reliance
U2 Authority / Payment
U3 Market Specs (
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights,
U7 Ext. Limit Spec.)
Bank CA Signature
Retrieve & Verify
Mkt. Okay? Check:
E2, M*, U3 R4, P4, T1
Market Certificate
M1 Identity / Reliance
M2 Market Desc. Info
M3 Product Spec.
M4 Participant Spec.
M5 Trade / Match Rules
Regulatory CA Signature
Verify

FIGURE 4.

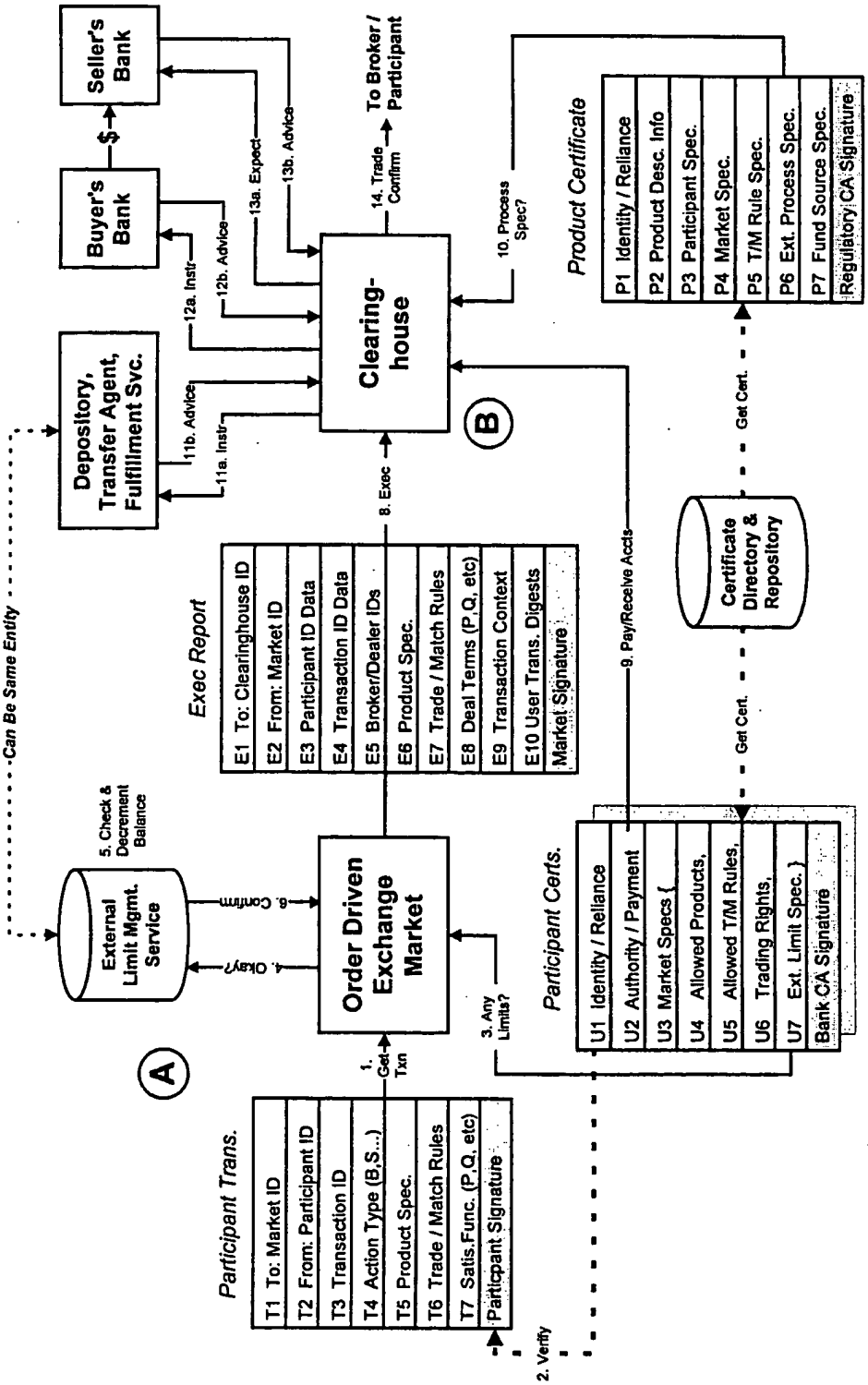

Seller's Bank
Buyer's Bank
$
To Broker / Participant
14. Trade Confirm
13a. Expect
13b. Advice
12a. Instr
12b. Advice
11b. Advice
11a. Instr
Depository, Transfer Agent, Fulfillment Svc.
Clearing-house
10. Process Spec?
Product Certificate
P1 Identity / Reliance
P2 Product Desc. Info
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
P6 Ext. Process Spec.
P7 Fund Source Spec.
Regulatory CA Signature
Can Be Same Entity
5. Check & Decrement Balance
External Limit Mgmt. Service
6. Confirm
4. Okay?
Order Driven Exchange Market
8. Exec
Exec Report
E1 To: Clearinghouse ID
E2 From: Market ID
E3 Participant ID Data
E4 Transaction ID Data
E5 Broker/Dealer IDs
E6 Product Spec.
E7 Trade / Match Rules
E8 Deal Terms (P,Q, etc)
E9 Transaction Context
E10 User Trans. Digests
Market Signature
9. Pay/Receive Accts
Certificate Directory & Repository
Get Cert.
Get Cert.
A
B
1. Get Txn
3. Any Limits?
Participant Trans.
T1 To: Market ID
T2 From: Participant ID
T3 Transaction ID
T4 Action Type (B,S...)
T5 Product Spec.
T6 Trade / Match Rules
T7 Satis.Func. (P,Q, etc)
Participant Signature
Participant Certs.
U1 Identity / Reliance
U2 Authority / Payment
U3 Market Specs {
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights,
U7 Ext. Limit Spec. }
Bank CA Signature
2. Verify

FIGURE 5.

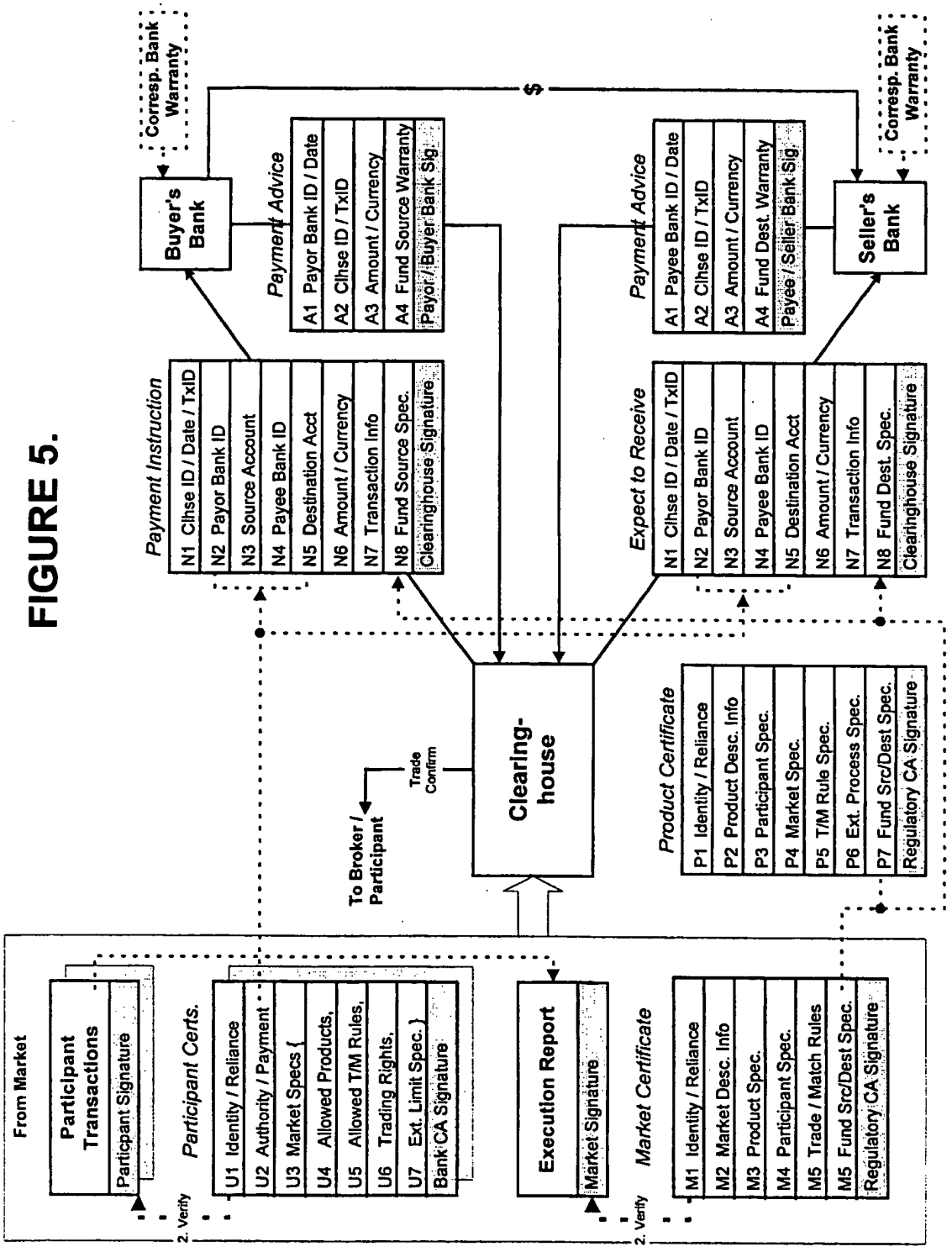

From Market
Participant Transactions
Particpant Signature
2. Verify
Participant Certs.
U1 Identity / Reliance
U2 Authority / Payment
U3 Market Specs {
U4 Allowed Products,
U5 Allowed T/M Rules,
U6 Trading Rights,
U7 Ext. Limit Spec. }
Bank CA Signature
Execution Report
Market Signature
2. Verify
Market Certificate
M1 Identity / Reliance
M2 Market Desc. Info
M3 Product Spec.
M4 Participant Spec.
M5 Trade / Match Rules
M5 Fund Src/Dest Spec.
Regulatory CA Signature
To Broker / Participant
Trade Confirm
Clearing-house
Product Certificate
P1 Identity / Reliance
P2 Product Desc. Info
P3 Participant Spec.
P4 Market Spec.
P5 T/M Rule Spec.
P6 Ext. Process Spec.
P7 Fund Src/Dest Spec.
Regulatory CA Signature
Payment Instruction
N1 Clhse ID / Date / TxID
N2 Payor Bank ID
N3 Source Account
N4 Payee Bank ID
N5 Destination Acct
N6 Amount / Currency
N7 Transaction Info
N8 Fund Source Spec.
Clearinghouse Signature
Expect to Receive
N1 Clhse ID / Date / TxID
N2 Payor Bank ID
N3 Source Account
N4 Payee Bank ID
N5 Destination Acct
N6 Amount / Currency
N7 Transaction Info
N8 Fund Dest. Spec.
Clearinghouse Signature
Buyer's Bank
Seller's Bank
Corresp. Bank Warranty
Corresp. Bank Warranty
$
Payment Advice
A1 Payor Bank ID / Date
A2 Clhse ID / TxID
A3 Amount / Currency
A4 Fund Source Warranty
Payor / Buyer Bank Sig
Payment Advice
A1 Payee Bank ID / Date
A2 Clhse ID / TxID
A3 Amount / Currency
A4 Fund Dest. Warranty
Payee / Seller Bank Sig

FIGURE 6.

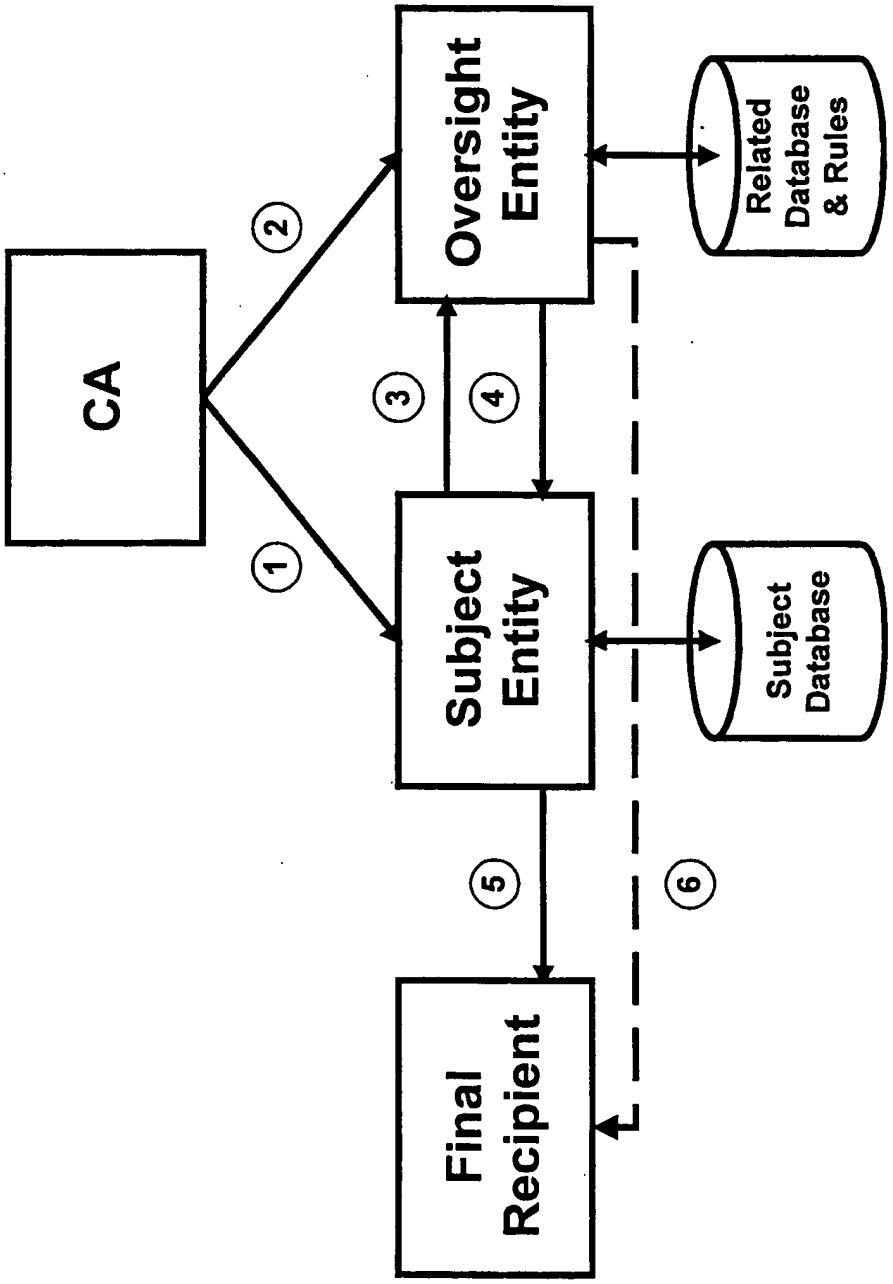

CA
Oversight Entity
Related Database & Rules
Subject Entity
Subject Database
Final Recipient
1
2
3
4
5
6

FIGURE 7.

(prior art)

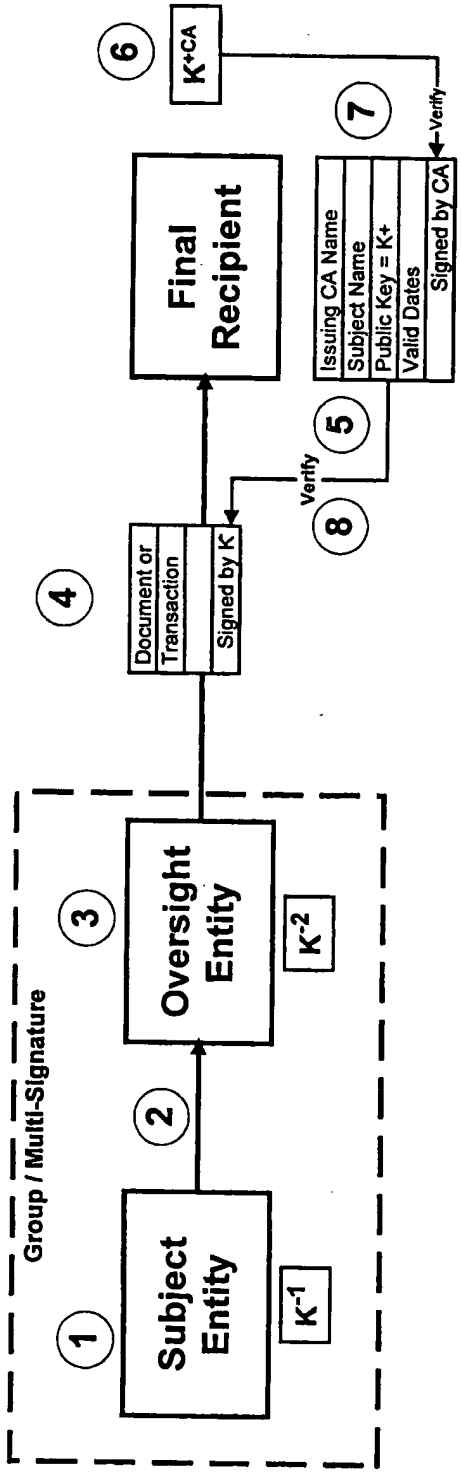


FIGURE 8.

(prior art)

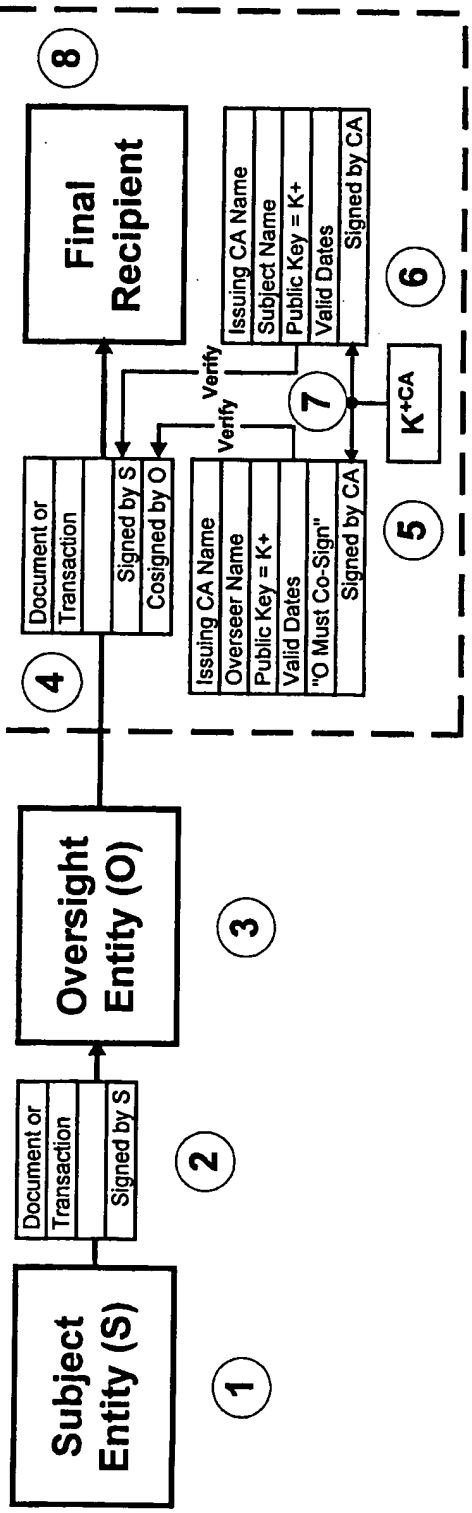


FIGURE 9.

(prior art)

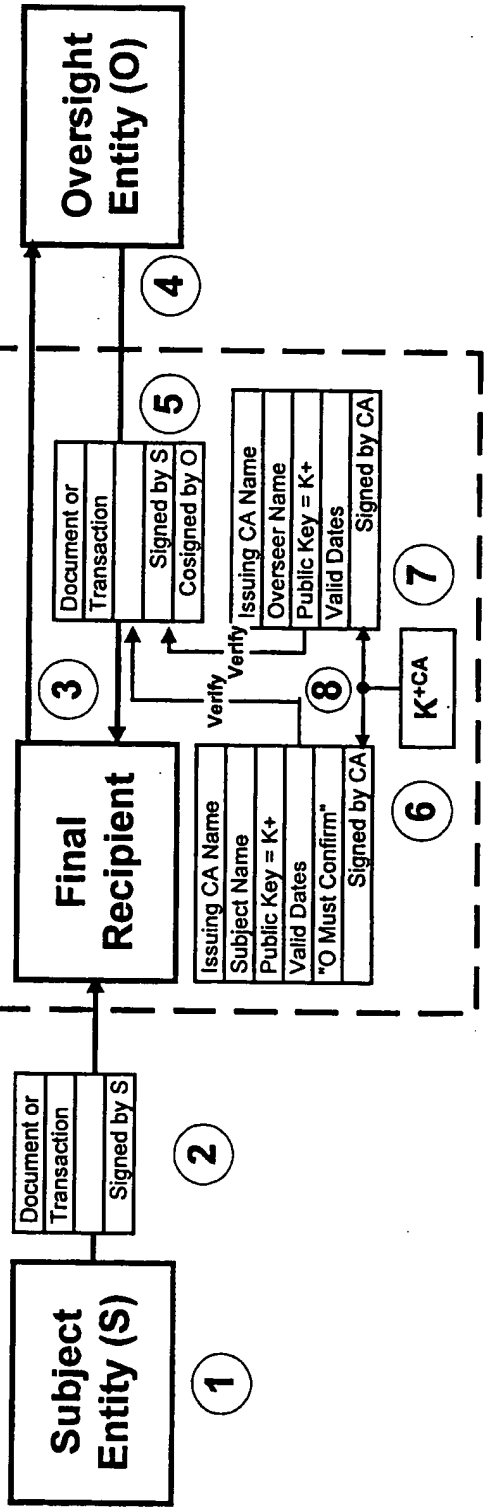
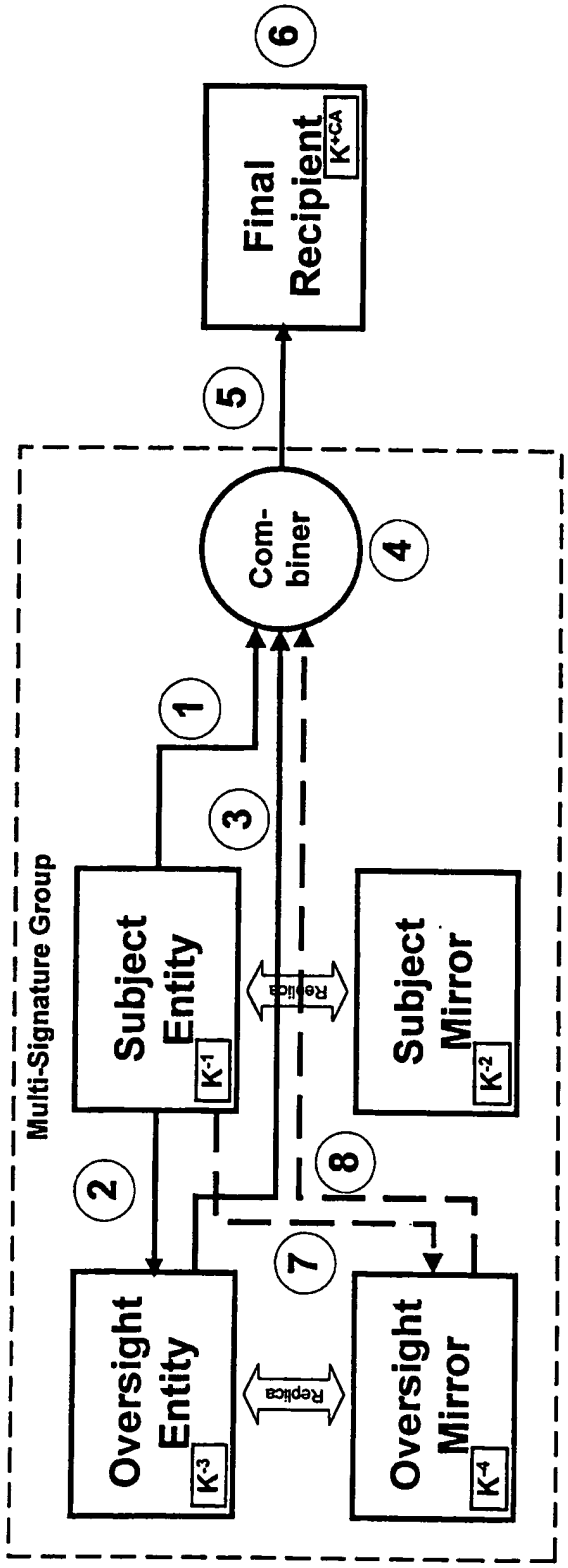


FIGURE 10.


Multi-Signature Group
Subject Entity
K-1
Subject Mirror
K-2
Oversight Entity
K-3
Oversight Mirror
K-4
Replica
Replica
Com-biner
Final Recipient
K+CA
1
2
3
4
5
6
7
8